INFORME 8

PRUEBA DE ANALISISIS FORENESE DIGITAL CON AUTOPSY Y FTK IMAGER

ESTUDIANTE:

SANTIAGO QUINTO COPETE

UNIVERSIDAD TECNOLOGICIA DEL CHOCÓ “DIEGO LUIS CORDOBA”

INGENERIA EN SISTEMA DE TELECOMUNICACIONES E INFORMATICA

QUIDBO-CHOCÓ

2025-1

INFORME 8

PRUEBA DE ANALISISIS FORENESE DIGITAL CON AUTOPSY Y FTK IMAGER

ESTUDIANTE:

SANTIAGO QUINTO COPETE

DOCENTE:

RAFAEL SANDOVAL MORALES

ASIGNATURA:

SEGURIDAD Y AUDITORIA DE REDES

UNIVERSIDAD TECNOLOGICIA DEL CHOCÓ “DIEGO LUIS CORDOBA”

INGENERIA EN SISTEMA DE TELECOMUNICACIONES E INFORMATICA

QUIDBO-CHOCÓ

2025-1

Tabla de contenido

LA TABLA DE ILUSTRACION

1 INTRODUCCION

El presente informe tiene como finalidad documentar el proceso de análisis forense digital realizado utilizando las herramientas **Autopsy** y **FTK Imager**, en los entornos **Kali Linux** y **Windows**, respectivamente. A través de esta práctica, se buscó comprender y aplicar los procedimientos técnicos para la **adquisición, preservación y análisis de evidencias digitales**, garantizando la integridad de la información.

El ejercicio permitió desarrollar competencias en el manejo de herramientas profesionales de informática forense, mediante la creación y verificación de imágenes digitales, el cálculo de valores hash y la interpretación de resultados obtenidos de dispositivos de almacenamiento. Además, se aplicaron principios de la cadena de custodia digital, asegurando la validez y trazabilidad de la evidencia examinada.

2 ALCANCE

Esta práctica abarca el proceso completo de análisis forense digital de una **memoria USB** de 3.74 GB, desde su identificación en el sistema operativo Kali Linux hasta su examen detallado con FTK Imager en Windows. Se realizaron tareas de clonación, generación de hash, creación de la imagen forense, y análisis de los datos recuperados.

El alcance incluye la documentación visual de cada fase, la verificación de integridad, y la comparación cruzada entre los resultados de **Autopsy** y **FTK Imager**, demostrando la validez del proceso y su utilidad en investigaciones digitales o auditorías de seguridad informática.

3 OBJETIVO

3.1 OBJETIVO GENERAL

Realizar un **análisis forense digital completo** de una memoria USB utilizando las herramientas **Autopsy** y **FTK Imager**, aplicando los principios técnicos y metodológicos de la informática forense para la preservación, extracción y análisis de evidencias digitales.

3.2 OBEJTIVO ESPECIFICOS

- Identificar y montar el dispositivo USB en el entorno Kali Linux para su posterior análisis.
- Calcular el valor hash del dispositivo y generar una imagen forense con el comando `dd`.
- Importar y examinar la imagen forense en **Autopsy**, analizando metadatos, archivos ocultos y registros de usuario.
- Verificar la integridad de la evidencia mediante FTK Imager en entorno **Windows**.
- Comparar los resultados obtenidos en ambas herramientas y validar la coherencia de los análisis realizados.

4 PRIMERO CAPITULO

4.1 MEMORIA USB

Observe esta imagen se conecta la memoria **USB modelo MICRO HC RNL AS-98** al sistema Kali Linux, con el fin de iniciar el análisis forense digital. El sistema reconoce la memoria con una capacidad aproximada de 3.74 GB, permitiendo verificar que está correctamente montada en el entorno. Este paso es fundamental, ya que se establece la base para la obtención de la evidencia digital sin alterar su contenido original, cumpliendo los principios de integridad forense.

Ilustración 1 Memoria USB conectada a Kali Linux

4.2 PRUEBA DE AUDITORIA INFORMATICA MEDIANTE AUTOPSY EN KALI LINUZ

Se ejecuta el comando lsblk en la terminal de Kali Linux para identificar las unidades de almacenamiento conectadas. Este comando permite verificar la ruta del dispositivo USB, generalmente asignada como /dev/sdb. La identificación correcta garantiza que el proceso de duplicación se realice sobre la memoria indicada y no sobre otro medio. Esta etapa evita errores de manipulación y asegura que la evidencia se mantenga intacta antes de proceder con el cálculo de hash.

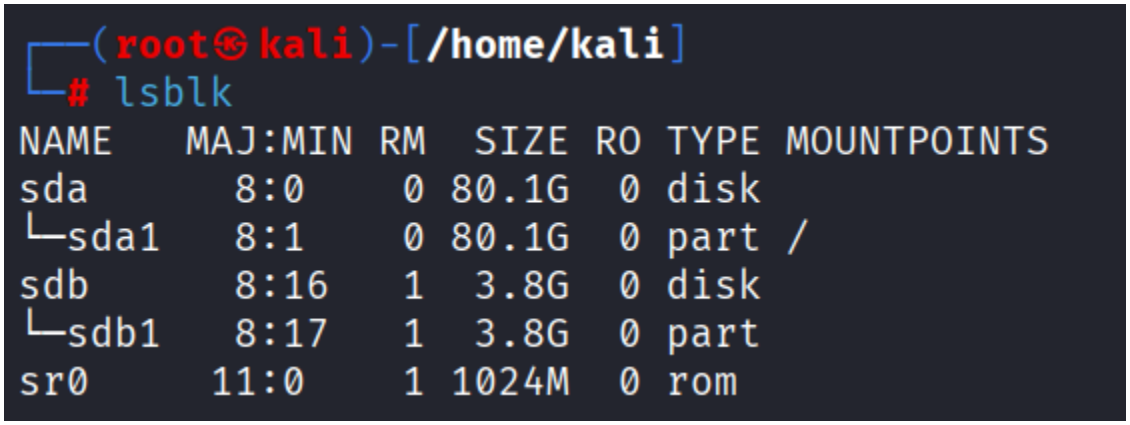


Ilustración 2 etección del dispositivo mediante comando lsblk

A continuación, se revisa la información del dispositivo mediante comandos como **fdisk -l**, confirmando la estructura de particiones de la memoria, este análisis inicial permite identificar el sistema de archivos y posibles sectores dañados, la información obtenida es clave para planificar la creación de la imagen forense completa, evitando omisiones o pérdidas de datos durante el proceso de copia, de esta forma, se garantiza una lectura precisa y sin errores de la evidencia digital.

```
┌──(root㉿kali)-[/home/kali]
└─# fdisk -l
Disk /dev/sda: 80.09 GiB, 86000000000 bytes, 167968750 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x06c77605

Device     Boot Start       End   Sectors  Size Id Type
/dev/sda1  *     2048 167968749 167966702 80.1G 83 Linux


Disk /dev/sdb: 14.65 GiB, 15728640000 bytes, 30720000 sectors
Disk model: UDisk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00129bac

Device     Boot    Start      End  Sectors  Size Id Type
/dev/sdb1  *        2048 30717879 30715832 14.6G  7 HPFS/NTFS/exFAT
/dev/sdb2       30717880 30719927     2048    1M  e W95 FAT16 (LBA)
```

Ilustración 3 Verificación de particiones del dispositivo USB.

En este paso se ejecuta el comando sha1sum /dev/sdb > /home/Desktop/hash.forense.sha1 para generar el hash único del dispositivo. Este valor funciona como una huella digital que permite verificar la autenticidad e integridad de los datos. Si el valor hash cambia en cualquier momento, significaría que la evidencia ha sido

alterada. Por ello, registrar este valor antes de copiar los datos es una práctica esencial en cualquier procedimiento de análisis forense digital.

Ilustración 4 Cálculo del hash SHA1 de la memoria.

La terminal muestra el código hash generado, en este caso **c6c023b508f9c1366a43bd72bc8519abf1e8eaed**, correspondiente a la memoria USB analizada. Este valor se almacena en un archivo denominado hash.forense.sha1 para futuras comparaciones. La generación y conservación de este hash constituye una evidencia fundamental en la cadena de custodia digital, pues garantiza que las copias de trabajo que se realizarán posteriormente serán fieles al dispositivo original sin ninguna modificación.

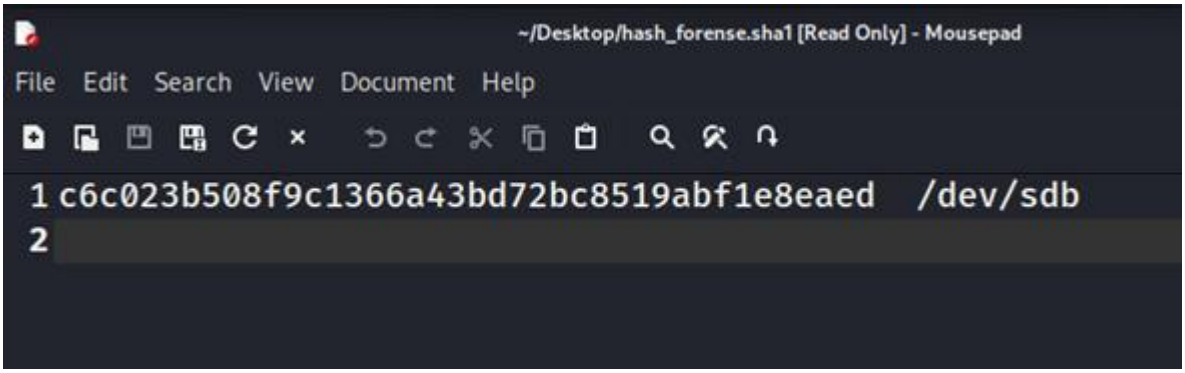


Ilustración 5 Resultado del hash generado en el sistema

Se utilizó el comando dd en Kali Linux para crear una imagen forense del dispositivo USB (/dev/sdb). El archivo resultante, imagen_usb_forense.dd, fue guardado en el escritorio.

Se emplearon las opciones noerror,sync para evitar interrupciones por errores de lectura. Se copiaron 4 GB en aproximadamente 20 minutos a 3.4 MB/s.

```
┌──(root㉿kali)-[/home/kali]
└─# dd if=/dev/sdb of=/home/kali/Desktop/imagen_usb_forense.dd
 conv=noerror,sync
7866368+0 records in
7866368+0 records out
4027580416 bytes (4.0 GB, 3.8 GiB) copied, 1180.72 s, 3.4 MB/s
```

Ilustración 6 Creación de la imagen forense con el comando dd

En esta etapa, el sistema Kali Linux muestra el progreso de la creación de la imagen forense, la operación puede tardar dependiendo de la capacidad del dispositivo y de la cantidad de información contenida. Es importante no interrumpir este proceso para evitar una copia incompleta. Una vez finalizado, se obtiene una imagen digital exacta del dispositivo, que podrá analizarse en entornos controlados sin comprometer la integridad de la evidencia original.

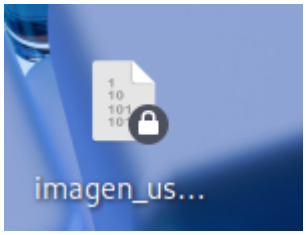


Ilustración 7 Proceso de clonación de datos en ejecución.

Concluida la clonación, se verifica que el archivo **imagen_usb_forense.dd** se haya creado correctamente en el escritorio de Kali Linux. Se comprueba su tamaño, fecha de

creación y permisos de acceso. Este paso asegura que la imagen sea completa y utilizable en las herramientas de análisis. La imagen servirá como copia maestra para Autopsy y FTK Imager, permitiendo investigar sin alterar la memoria original, respetando las normas del análisis forense digital.

```
┌──(root㉿kali)-[/home/kali]
└─# sha1sum /home/kali/Desktop/imagen_usb_forense.dd
7c1d1d9ef39e1effd9f498af4a28f1e7ee1b6aab  /home/kali/Desktop/imagen_usb
_forense.dd
```

Ilustración 8 Verificación de la imagen forense creada.

Para garantizar que la imagen forense sea idéntica al dispositivo físico, se calcula nuevamente un hash SHA1 sobre el archivo generado. Luego, se compara con el hash original obtenido del dispositivo. Si los valores coinciden, se confirma que la imagen fue creada correctamente y sin modificaciones. Este procedimiento es esencial en toda investigación digital, ya que proporciona trazabilidad y autenticidad a los datos obtenidos para análisis posteriores en entornos controlados.

Ilustración 9 Cálculo de hash de la imagen generada.

Luego salimos en la terminal en Kali Linux, buscaremos en el buscador luego colocamos en el nombre de la app para poder hacer el proceso

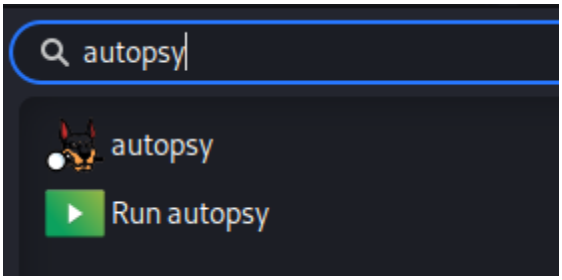


Ilustración 10 Preparación del entorno en Kali Linux

Veamos en esta ventanita, se lo está pidiendo la clave en Kali Linux para poder seguir con el proceso que vamos a desarrollar, ya que la versión tiene como 2.24 en la versión se actualizaron en el anteriormente.

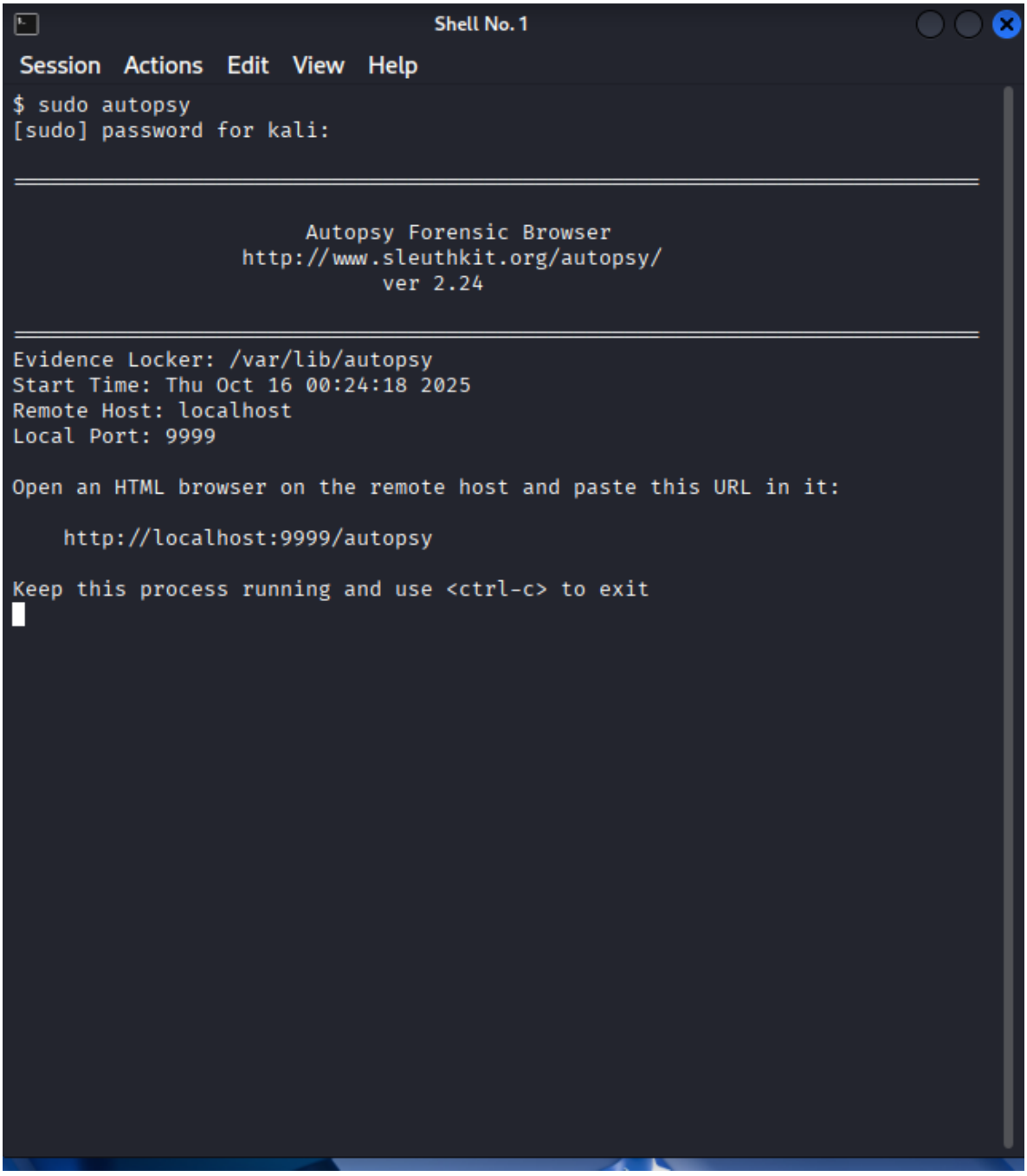


Ilustración 11 El comando que se abrio el autopsy

Después de eso le daremos en el enlace donde dice http://localhost:9999/autopsy, le daremos en la tecla con el **control + mouse izquierdo** o le dará el mouse derecho de, se abrirá en una ventanita de la página de **autopsy.**

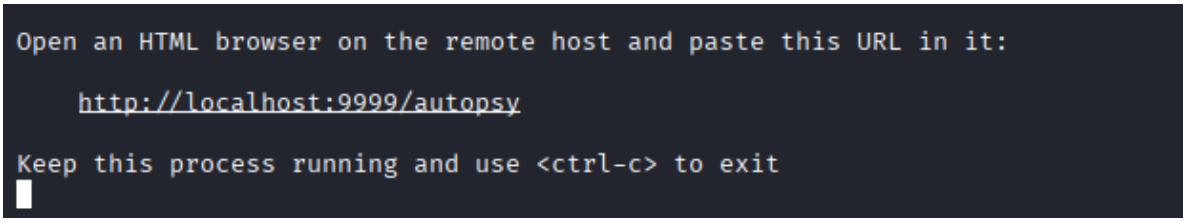


Ilustración 12 enlace de autopsy

5 LA PAGINA DE AUTOPSY

5.1 INTERFAZ INICIAL DEL PROGRAMA AUTOPSY FORENSE BROWSER 2.24

Se abrió muestra la ventana principal del programa **Autopsy Forensic Browser en su versión 2.24.** Desde esta interfaz se puede crear un nuevo caso forense o abrir uno existente para continuar el análisis. El aviso de seguridad recomienda desactivar JavaScript para evitar vulnerabilidades durante la investigación. Esta pantalla marca el inicio formal del entorno de trabajo, donde se gestionarán las evidencias digitales, los reportes y los módulos de análisis dentro del flujo del proceso forense digital.

Ilustración 13 Interfaz inicial del programa Autopsy

5.2 CREACION DE UN NUEVO CASO FORENSE EN AUTOPSY

Veamos el siguiente paso, En este paso se configura un nuevo caso en Autopsy, ingresando el nombre del proyecto, la descripción y los datos del investigador responsable, el caso se denomina **MiPrimercaso-1** y el investigador asignado es **Quintocopetesantiago**. Esta información permite organizar las evidencias y resultados dentro del entorno forense, asegurando trazabilidad y control del proceso, una vez completados los campos, se procede con la **creación del caso (new case)** para iniciar la fase de incorporación de la evidencia digital.

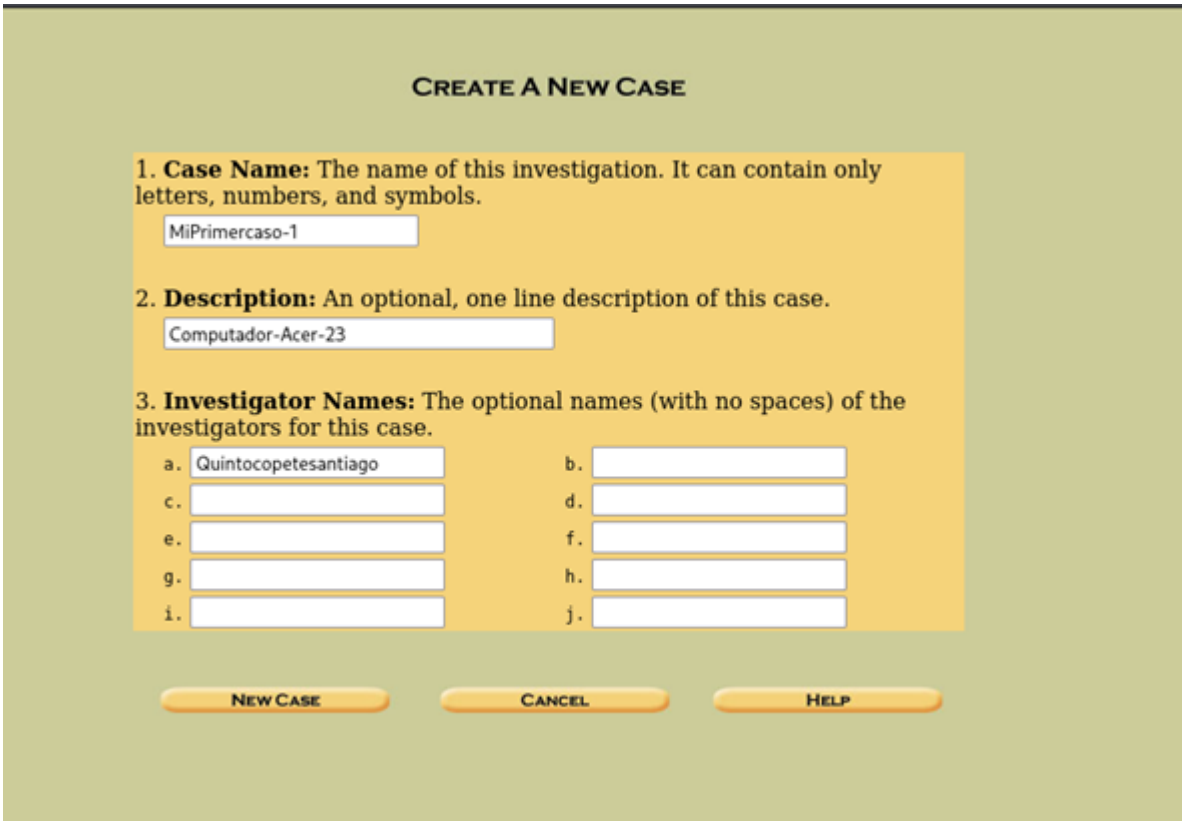


Ilustración 14 Creación de un nuevo caso en Autopsy.

5.3 CONFIRMACION DECREACION DEL CASO E INICIO DE CONFIGURACION DEL HOST

Veamos en esta ventana Autopsy confirma la creación del caso **MiPrimercaso-1**, generando el directorio correspondiente y el archivo de configuración en el sistema. A continuación, se solicita la selección del investigador responsable, en este caso **Quintocopetesantiago**, antes de proceder con la adición del host que contendrá la evidencia digital. Este paso asegura que el caso quede correctamente asociado al analista designado, garantizando organización, trazabilidad y control dentro de la estructura del proyecto forense y luego le da **ADD HOST.**

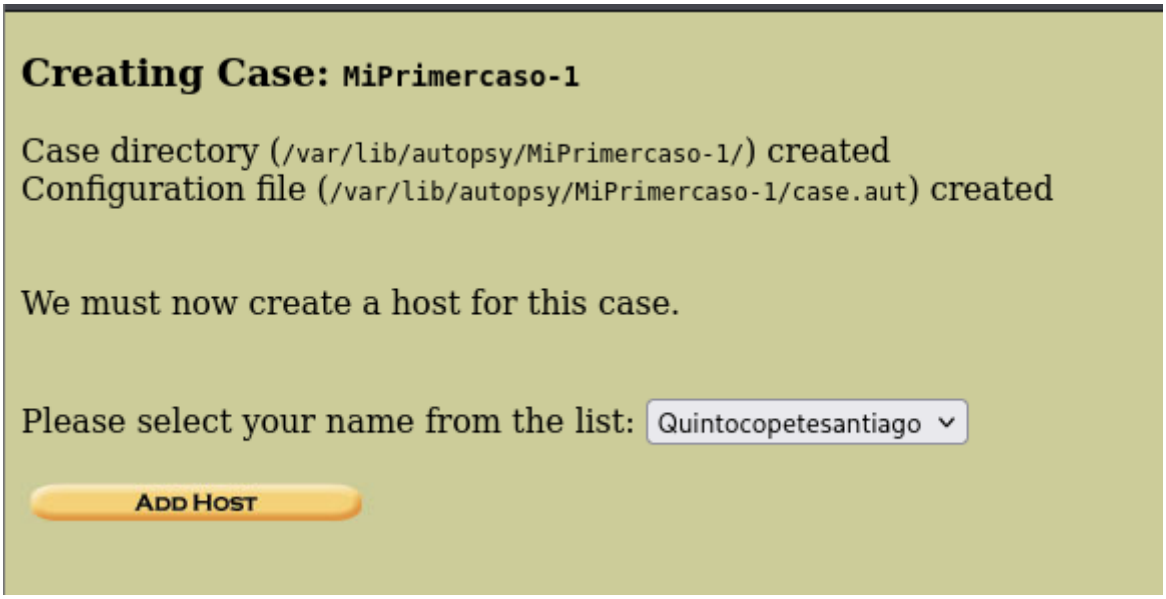


Ilustración 15 Creacion de un caso

5.4 ADICION DEL HSOT AL CASO FORENSE EN AUTOPSY

En este paso se agrega el host denominado **MVKaliPITTI1-1** al caso forense **MiPrimercaso-1.** El sistema Autopsy crea de forma automática el directorio del host y su archivo de configuración correspondiente, almacenando la estructura necesaria para registrar la evidencia digital. Este procedimiento es esencial para mantener la organización del caso y

separar las fuentes de datos analizadas. Con el host configurado, el analista puede importar la imagen forense del dispositivo a examinar, por último, le daremos clic **ADD IMAGEN**

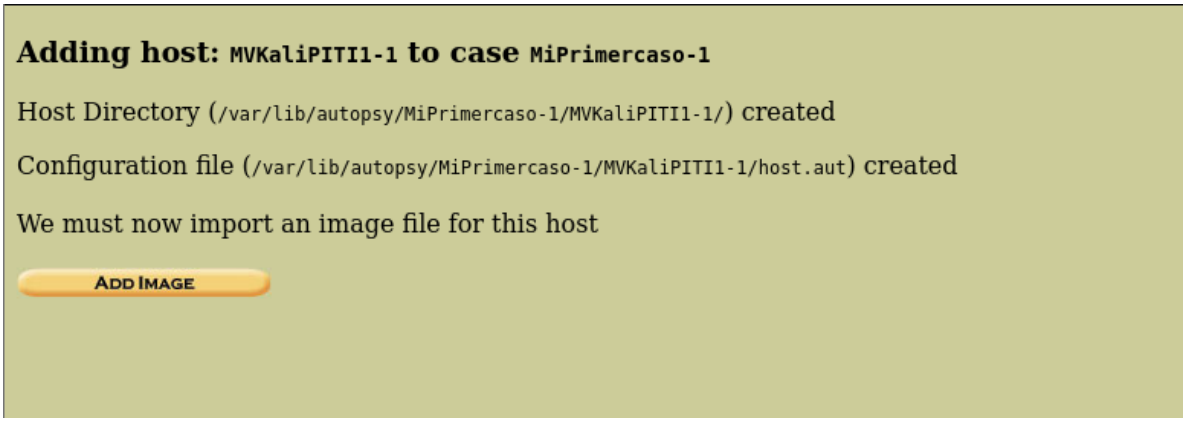


Ilustración 16 Adición del host en Autopsy

5.5 INTERFAZ PARA LA IMPORTACION DE LA IMAGEN FORENSE

Veamos el siguiente paso se muestra la ventana del host MVKaliPITTI1-1 dentro del caso MiPrimercaso-1, donde aún no se ha añadido ninguna imagen forense. El sistema ofrece la opción **Add Image File** para importar la evidencia digital a analizar. Esta pantalla es crucial, ya que permite al investigador cargar copias exactas de dispositivos o particiones sin alterar los datos originales, garantizando la integridad del proceso forense. Desde aquí también se accede a módulos de verificación e integridad.

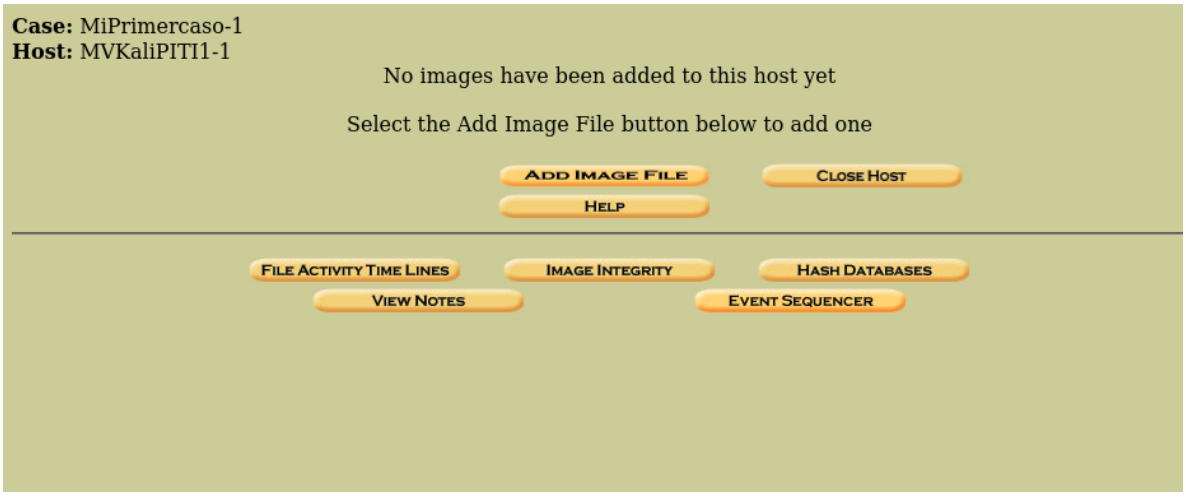


Ilustración 17 Interfaz para añadir la imagen forense.

5.6 CONFIGURACION DE LA IMPORTACION DE LA IMAGEN FORENSE

Veamos el siguiente, se define la ruta del archivo de imagen forense dentro del sistema, en este caso **imagen_usb_forense.dd**, almacenado en el escritorio de Kali Linux. Además, se especifica que el tipo de imagen corresponde a un disco completo y que el método de importación será mediante un enlace simbólico (*symlink*), lo cual evita duplicar archivos innecesariamente. Este procedimiento garantiza una correcta incorporación de la evidencia digital manteniendo su integridad y estructura original durante el proceso de análisis forense, luego les daremos clic donde dice **NEXT**

Ilustración 18 Configuración de la imagen forense antes de su carga.

5.7 DETALLES Y ANALISIS DEL ARCHIVOS DE IMAGEN FORENSE.

Veamos en esta imagen se muestra la información detallada de la imagen forense **imagen_usb_forense.dd.** Se visualiza la opción de cálculo o verificación del hash MD5, una medida esencial para garantizar la integridad de los datos analizados. Además, se identifican las particiones contenidas en la imagen, destacando una de tipo **Win95 FAT32** con punto de montaje asignado a ***C:*** y un rango de sectores definidos. Esta información confirma que el archivo ha sido reconocido correctamente y que está listo para iniciar el proceso de análisis forense y luego les daremos clic **ADD.**

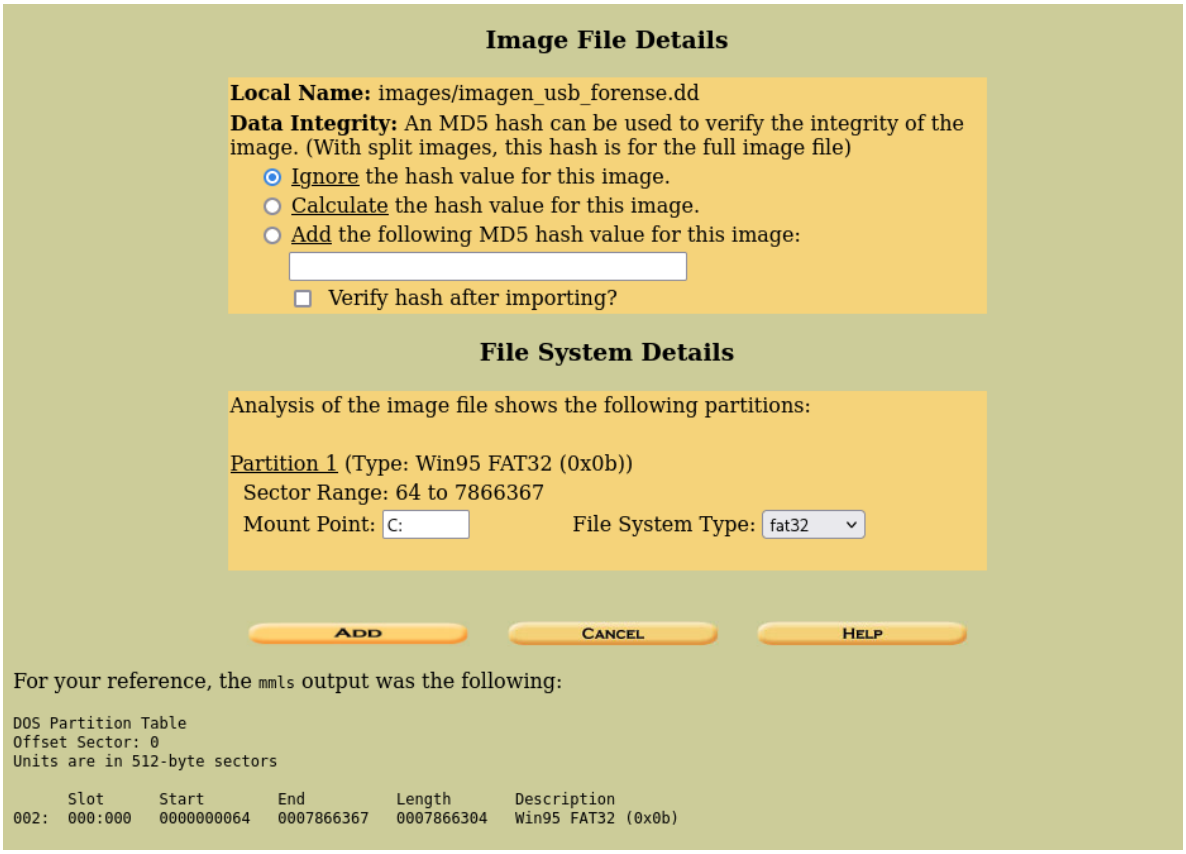


Ilustración 19 Verificación de la imagen forense y análisis de particiones

5.8 CONFIRMACION DE LA CARGA CORRECTAMENTE DE LA IMAGEN FORENSE

Pasamos al siguiente paso, Autopsy confirma que la imagen forense fue vinculada correctamente al *evidence locker* del caso *MiPrimercaso-1*. El sistema asigna identificadores únicos a los elementos agregados: *img1* para el archivo de imagen, *vol1* para la imagen de disco y *vol2* para la partición tipo *FAT32*. Esta confirmación es esencial, ya que garantiza que la evidencia digital fue incorporada con éxito, preservando su integridad y permitiendo continuar con el análisis detallado del contenido almacenado en el dispositivo investigado.

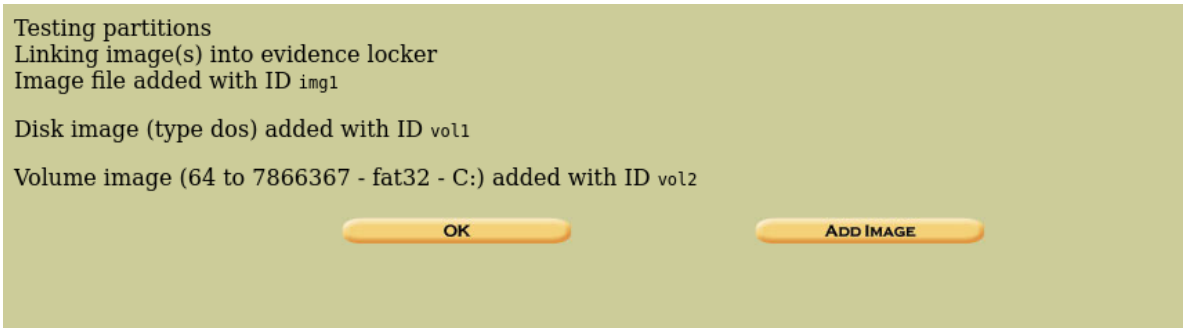


Ilustración 20 Confirmación de carga de la imagen forense en Autopsy.

5.9 VISUALIZACION DEL ARBOL DE DIRECTORIOS DE LA PARTICION

Una vez que la imagen forense ha sido cargada y validada, Autopsy permite al analista navegar por la estructura lógica de la partición (vol2 - FAT32). Esta imagen muestra el árbol jerárquico del sistema de archivos, revelando los directorios y archivos hallados. Esta vista es fundamental, ya que permite acceder a la información de manera detallada, seleccionar carpetas de interés y preparar la fase de búsqueda de archivos específicos (visibles, ocultos o eliminados), iniciando el análisis activo de la evidencia digital.

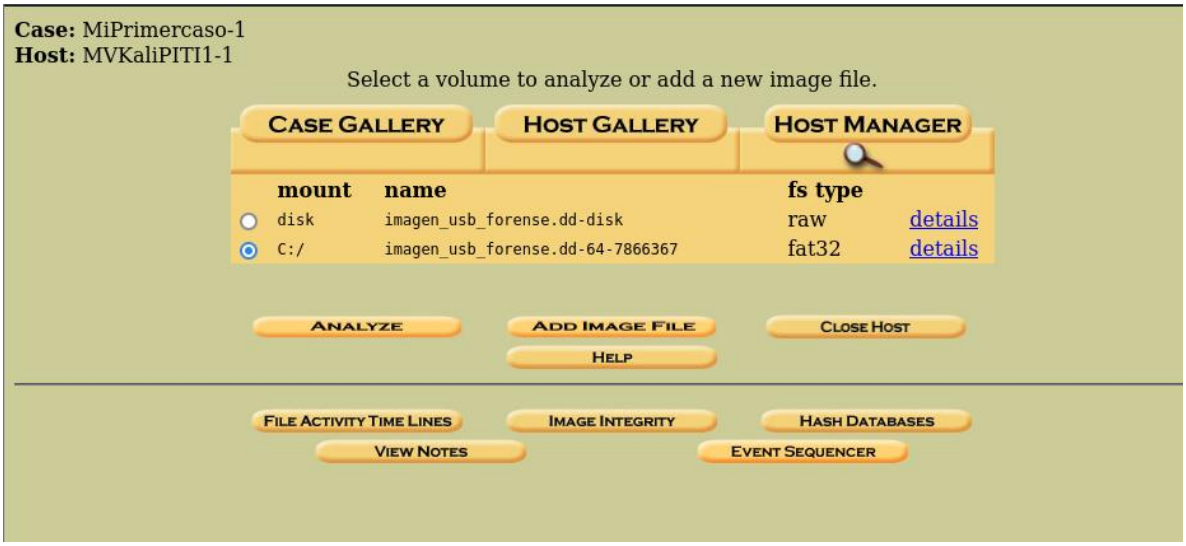


Ilustración 21 Visualización del árbol de directorios en Autopsy.

5.10 SELECCION DEL ARCHIVO DE IMAGEN FORENSE

se utiliza el explorador de archivos del sistema operativo para localizar y seleccionar la imagen forense previamente creada en Kali Linux, denominada imagen_usb_forense.dd. Este paso asegura que Autopsy apunte a la evidencia digital correcta. La selección del archivo es crítica, ya que se verifica que la imagen sea accesible y que corresponda al *hash* validado en la fase de adquisición, manteniendo la trazabilidad del medio digital que será objeto de análisis detallado.

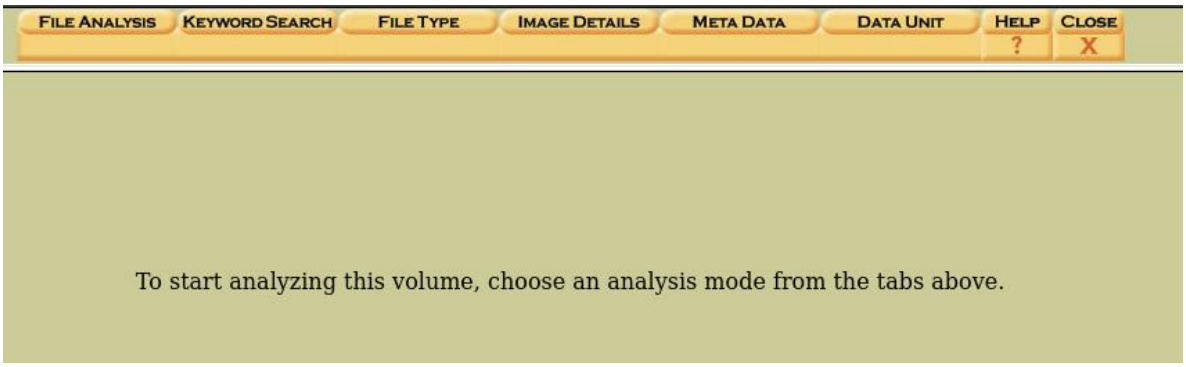


Ilustración 22 Selección de la imagen forense a importar.

5.11 VISUALIZACION DEL ARBOL DE DIRECTORIOS Y EXPLORACION DE ARCHIVOS

Una vez que la imagen forense ha sido cargada y procesada por Autopsy, esta imagen muestra la **navegación activa** dentro de la estructura de la partición FAT32. Se puede observar el panel de la izquierda con el árbol jerárquico de directorios y la lista de archivos en el panel central. Esta etapa marca el inicio del análisis exploratorio, donde el investigador puede acceder a archivos visibles y ocultos. Es crucial para identificar rutas de interés, clasificar el tipo de contenido y preparar la búsqueda de archivos eliminados o sospechosos, basándose en la estructura lógica del sistema de archivos.

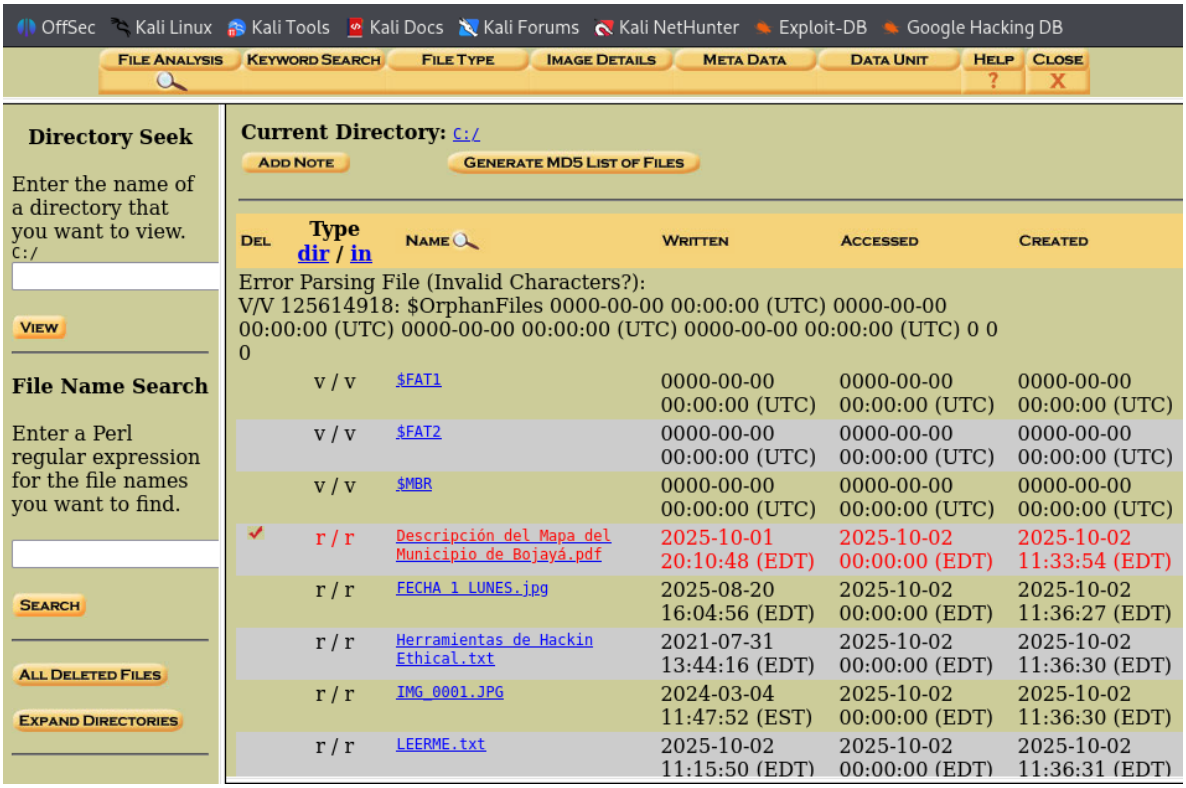
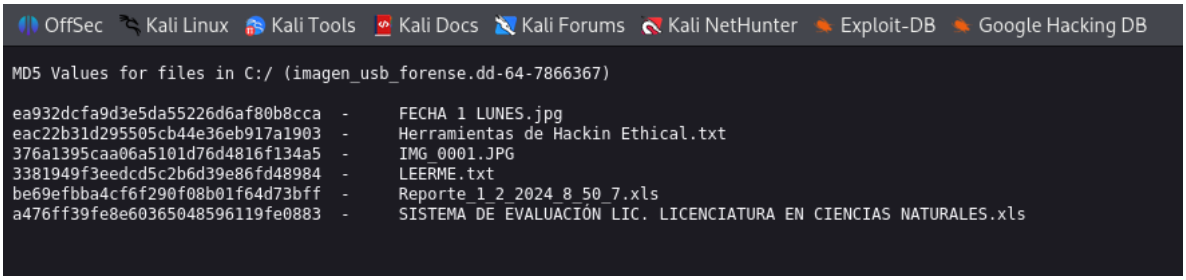


Ilustración 23 Visualización del árbol de directorios y contenido en Autopsy.

5.12 IDENTIFICACION Y RECUPERACUIB DE ARCHIVOS ELIMINADOS

Esta imagen documenta el hallazgo de archivos que fueron previamente borrados del dispositivo, pero que han sido identificados y recuperados por Autopsy gracias al análisis de

los sectores no sobrescritos de la imagen forense. Se observa un archivo eliminado (eliminados.txt) que ahora está disponible para inspección. La recuperación de estos elementos, junto con la verificación de sus fechas de creación y eliminación, es un proceso vital en la investigación forense, ya que permite obtener pruebas que el usuario pudo haber intentado ocultar o borrar intencionalmente.



6 SEGUNDO CAPITULO

7 PRUEBA DE AUDITORIA DE FORENSE INFORMATICA EN ENTORNO WINDOWS CON AUTOPSY

7.1 RESULTADO DE LA BUSQYEDA DE PALABRAS DE CLAVE DENTRO DE LA EVIDENCIA

La imagen muestra los resultados agrupados por palabras clave encontradas en la evidencia digital. Esta función es fundamental para **agilizar la identificación** de documentos, comunicaciones, o referencias que sean directamente relevantes para los objetivos de la investigación. Al automatizar la revisión de grandes volúmenes de texto, se facilita la localización de evidencia que de otra manera sería difícil de encontrar manualmente, fortaleciendo el informe forense con hallazgos puntuales.

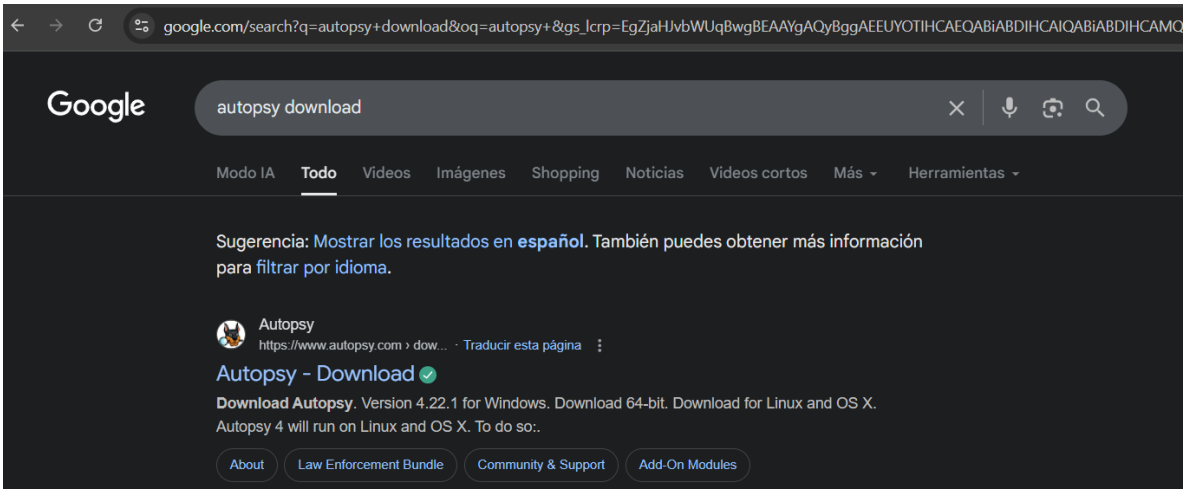


Ilustración 24 Resultados de la búsqueda de palabras clave en Autopsy.

7.2 REVISION Y VISUALIZACION DE DOCUMENTOS DE TEXTO Y ARCHIVOS PDF

Se inicia la segunda fase del proceso utilizando el software FTK Imager en Windows. Esta herramienta se emplea para examinar, visualizar y verificar imágenes forenses. Antes de comenzar, se configura el entorno de trabajo asegurando espacio de almacenamiento y permisos administrativos. FTK Imager complementa los resultados obtenidos con Autopsy, ofreciendo una vista más directa y detallada de la estructura del sistema de archivos, garantizando la integridad de la información a lo largo del proceso forense.

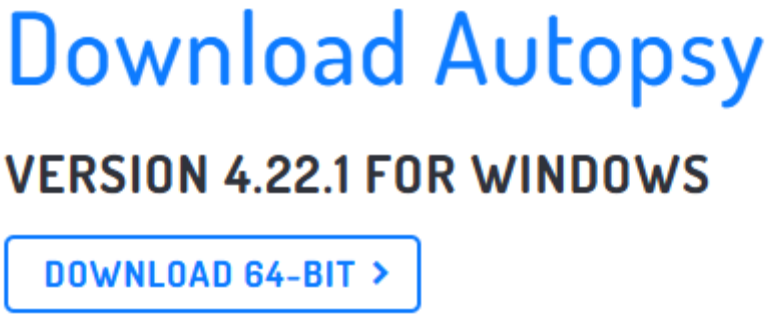


Ilustración 25 Instalación del software Autopsy en Windows.

Se descarga el instalador desde la página oficial de AccessData, asegurando una versión actualizada y libre de alteraciones. La procedencia oficial del software es importante para mantener la validez del análisis. Este paso también incluye la verificación de la integridad del instalador mediante su hash, garantizando que no haya sido modificado. Una vez completada la descarga, se prepara el entorno Windows para proceder con la instalación del programa forense utilizado en investigaciones digitales.

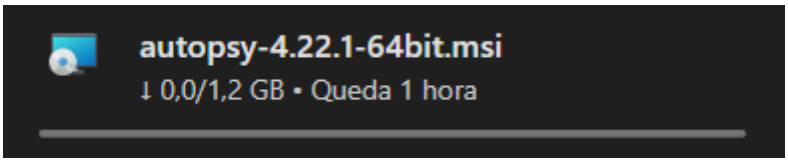


Ilustración 26 Primera ejecución de Autopsy..

Se ejecuta el instalador de FTK Imager, configurando el directorio de instalación y los módulos necesarios para el análisis. La instalación permite acceder a herramientas de creación de imágenes, cálculo de hash, exploración de archivos y generación de reportes. Una vez finalizado, el programa queda disponible en el menú principal del sistema operativo. FTK Imager es reconocido por su precisión y eficiencia en la obtención de información de medios digitales dentro de auditorías forenses profesionales.

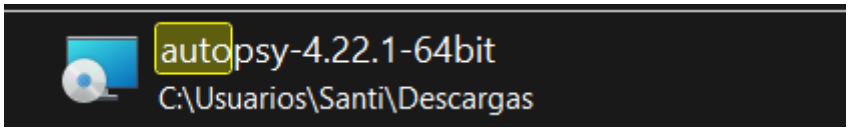


Ilustración 27 instalado completamente

Se abre el programa FTK Imager, mostrando su interfaz principal con las opciones de importar evidencias, visualizar estructuras de archivos y generar reportes. Desde este entorno, se pueden agregar imágenes forenses creadas previamente, incluyendo la obtenida

en Kali Linux. Su diseño intuitivo permite realizar un análisis rápido y ordenado, cumpliendo las normas de integridad y preservación de la evidencia digital en procesos de auditoría, investigación o prácticas de ciberseguridad aplicada en entornos académicos.

Ilustración 28 Autopsy está en el escritorio

Dentro de Autopsy se crea un nuevo caso forense con los datos del investigador y del dispositivo analizado. Se agrega la imagen imagen_usb_forense.dd como fuente de evidencia digital. El programa permite incluir varias imágenes o discos si la investigación lo requiere. Este proceso asegura que los resultados obtenidos queden organizados en carpetas específicas, permitiendo una trazabilidad clara de la información revisada durante toda la auditoría forense informática.

Ilustración 29 Creación de caso forense en Autopsy.

Antes de iniciar el procesamiento de la imagen, se seleccionan los módulos de análisis necesarios, como recuperación de archivos eliminados, búsqueda de palabras clave, extracción de metadatos y análisis de artefactos del sistema. Esta configuración permite personalizar el tipo de revisión según los objetivos de la investigación. Los módulos seleccionados se ejecutarán automáticamente, generando reportes detallados de las evidencias encontradas en la imagen forense importada desde Kali Linux.

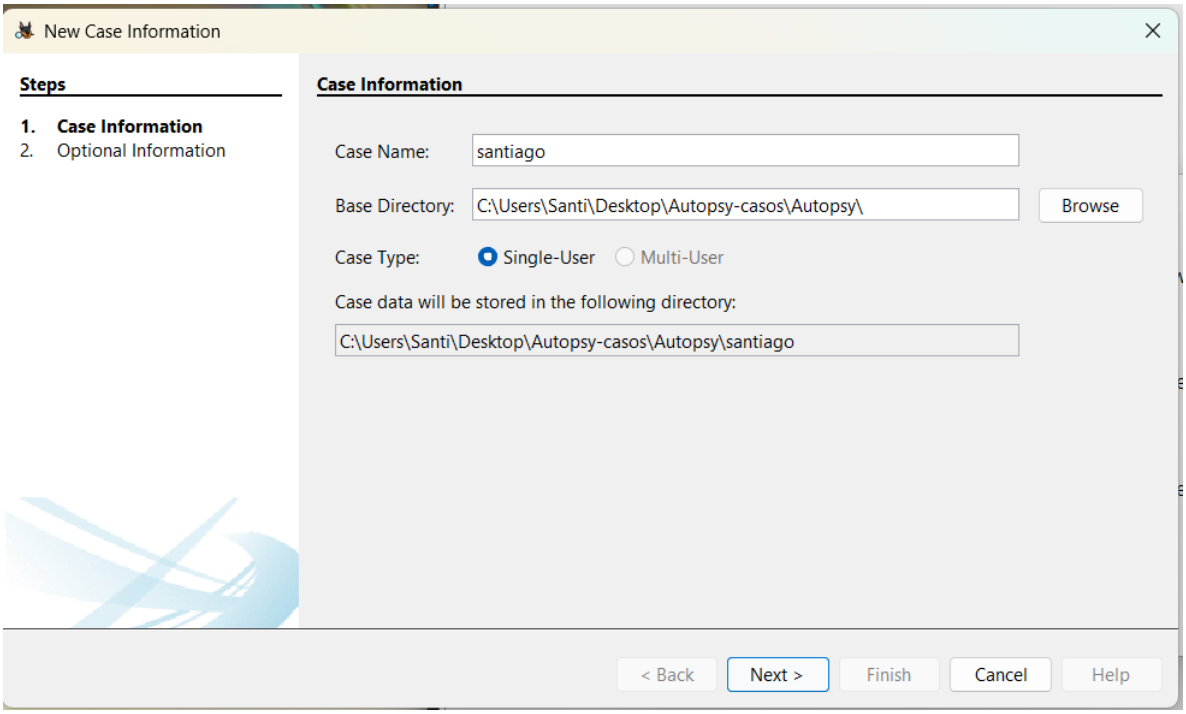


Ilustración 30 nuevo caso informacion

Autopsy comienza el análisis de la imagen forense. El sistema procesa la información en busca de artefactos, archivos sospechosos, registros de usuario y cualquier dato potencialmente útil. Durante este proceso se pueden detectar archivos borrados, documentos ocultos y metadatos relevantes. Este paso es fundamental para identificar comportamientos o acciones dentro del dispositivo, permitiendo reconstruir eventos y determinar posibles

irregularidades o evidencias que sustenten un caso de auditoría o investigación.

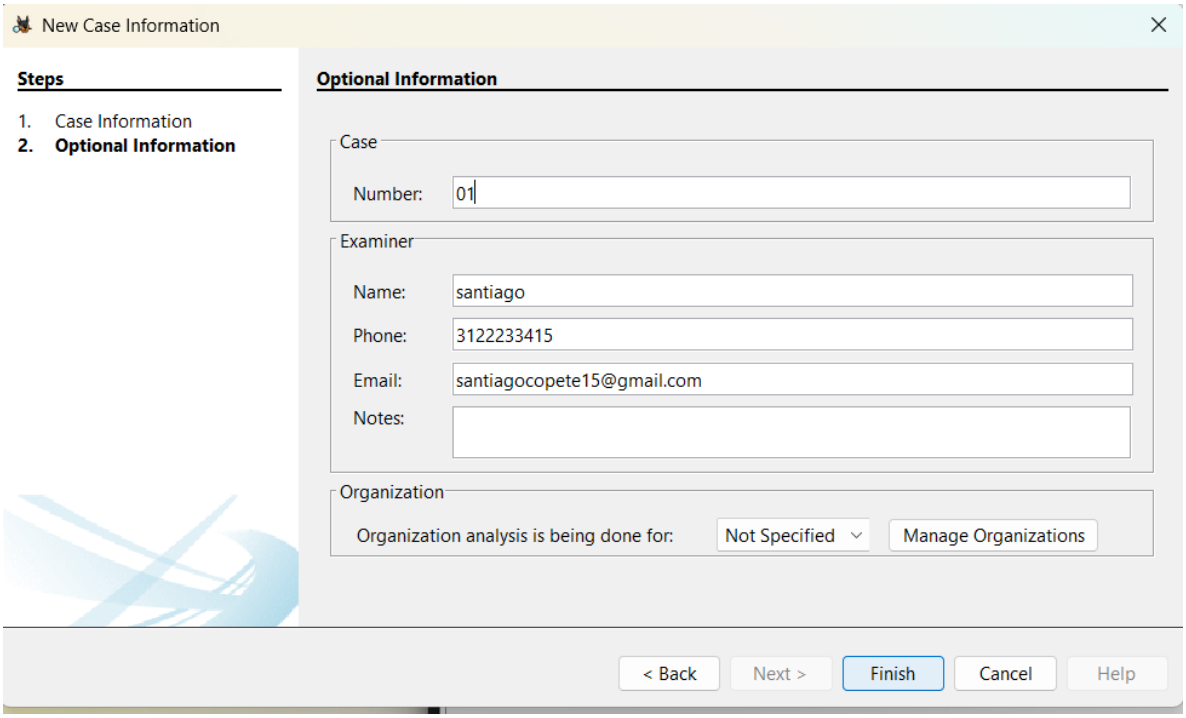


Ilustración 31 Creación de caso forense en Autopsy.

Una vez completado el análisis, Autopsy presenta un árbol jerárquico con todas las carpetas y archivos hallados en la imagen forense. Esta vista permite navegar por la estructura del dispositivo y acceder a la información de manera detallada. Se pueden visualizar archivos visibles, ocultos y eliminados, junto con sus propiedades. El investigador puede filtrar resultados según extensión o fecha, facilitando la localización de elementos que resulten

relevantes para la auditoría digital.

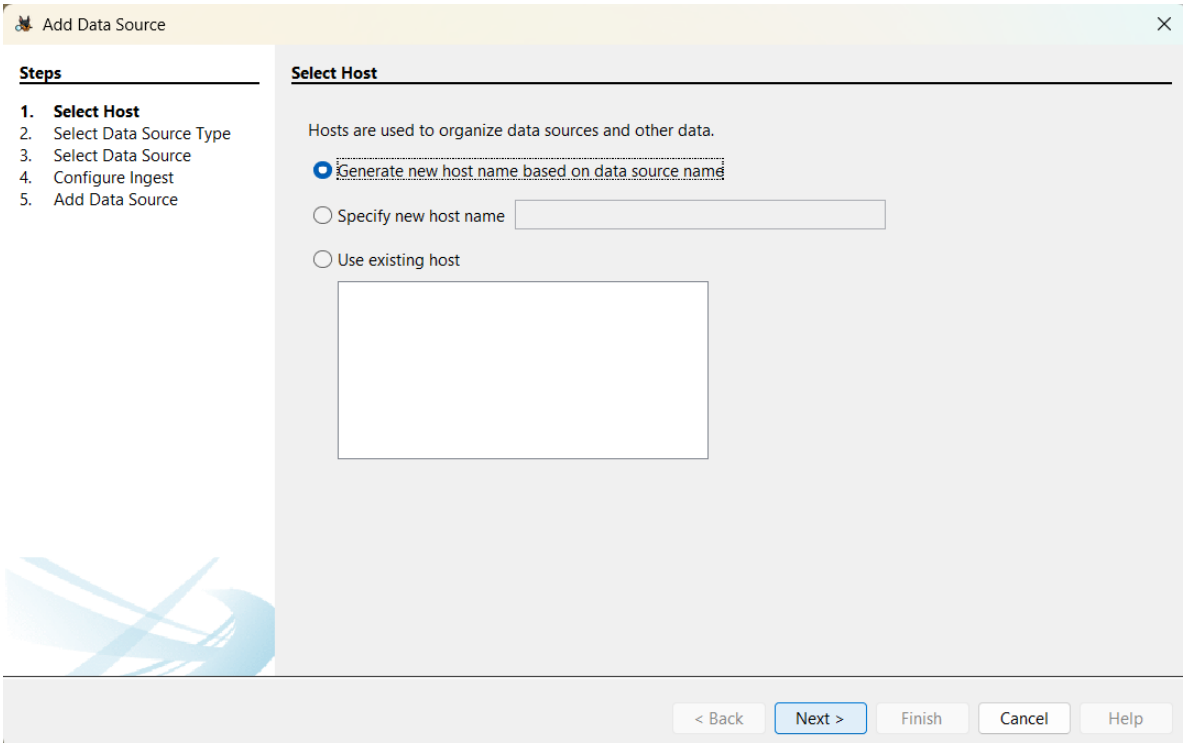


Ilustración 32 agregar fuente de datos

Autopsy identifica archivos eliminados que permanecen en los sectores no sobrescritos del dispositivo. Estos archivos son recuperados y almacenados temporalmente para su inspección. La herramienta muestra detalles como tamaño, tipo de archivo y fecha de modificación. Este proceso permite al investigador reconstruir evidencia que el usuario pudo haber intentado borrar, proporcionando información clave sobre la actividad previa en el sistema y fortaleciendo el análisis forense con resultados verificables y trazables.

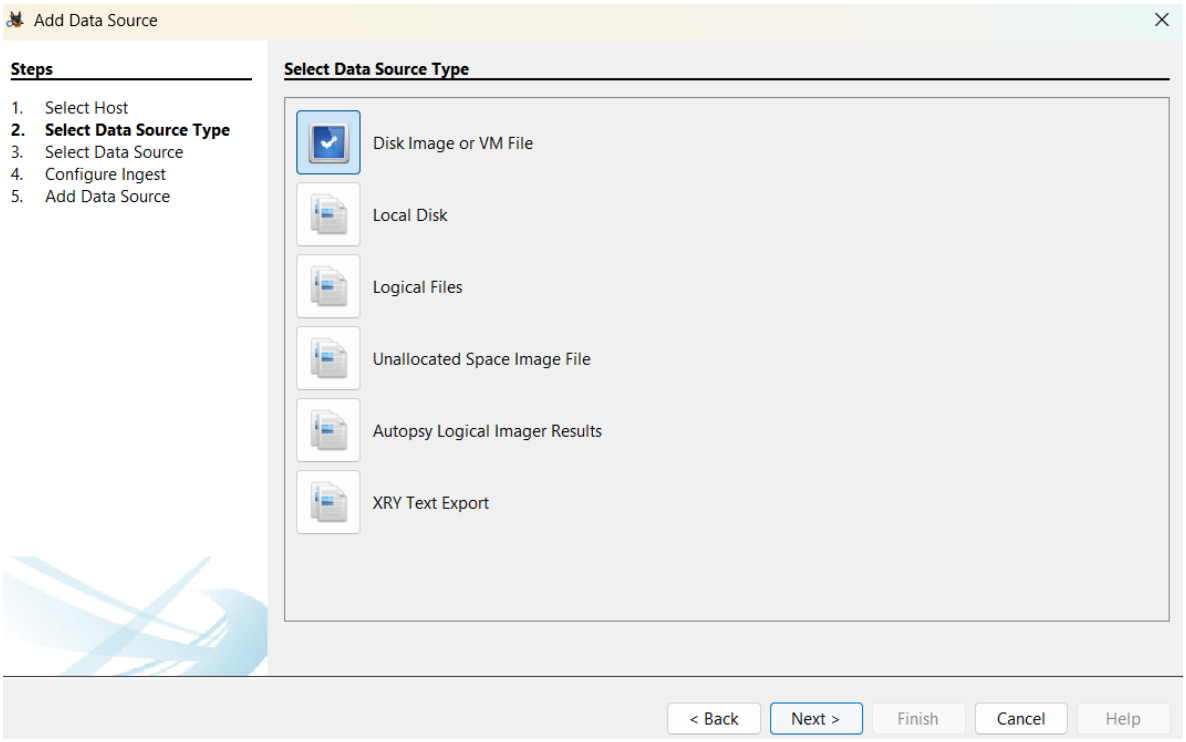


Ilustración 33 almacenamiento seguro del proyecto forense.

En esta etapa se examinan los metadatos de los archivos hallados: fechas de creación, modificación, acceso y usuario asociado. Estos datos son fundamentales para establecer líneas de tiempo en la investigación. Los metadatos permiten entender cuándo y cómo fue utilizada la memoria USB, así como identificar posibles manipulaciones. Autopsy facilita esta tarea mediante paneles de detalle que muestran información técnica de cada archivo analizado dentro de la evidencia digital procesada.

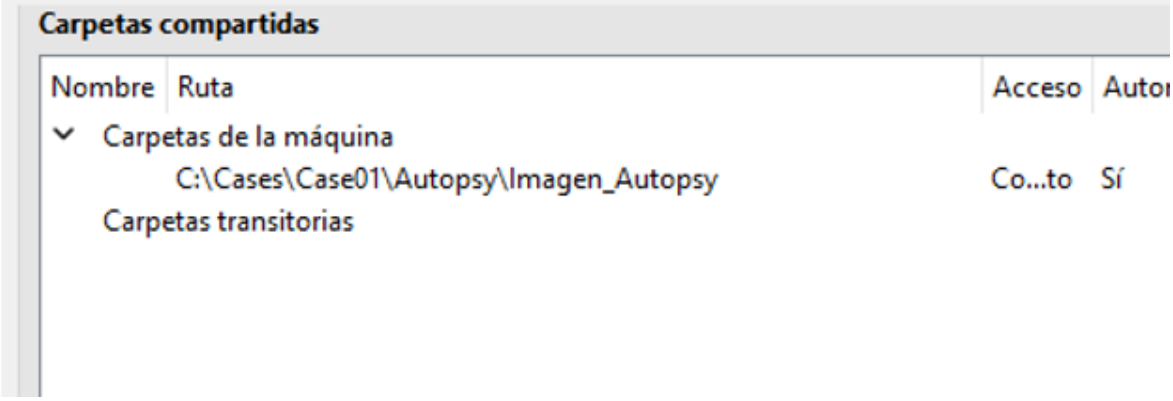


Ilustración 34 Carpeta compartidas en virtual box (Kali linux)

Se utiliza la función de búsqueda avanzada de Autopsy para localizar palabras clave relacionadas con la investigación, tales como nombres, fechas, direcciones o extensiones específicas. Esta función agiliza la identificación de documentos relevantes o comunicaciones potencialmente comprometedoras. Los resultados se agrupan automáticamente y pueden exportarse a reportes para documentar hallazgos específicos. Esta herramienta es esencial en auditorías donde se requiere analizar grandes volúmenes de información en poco tiempo.

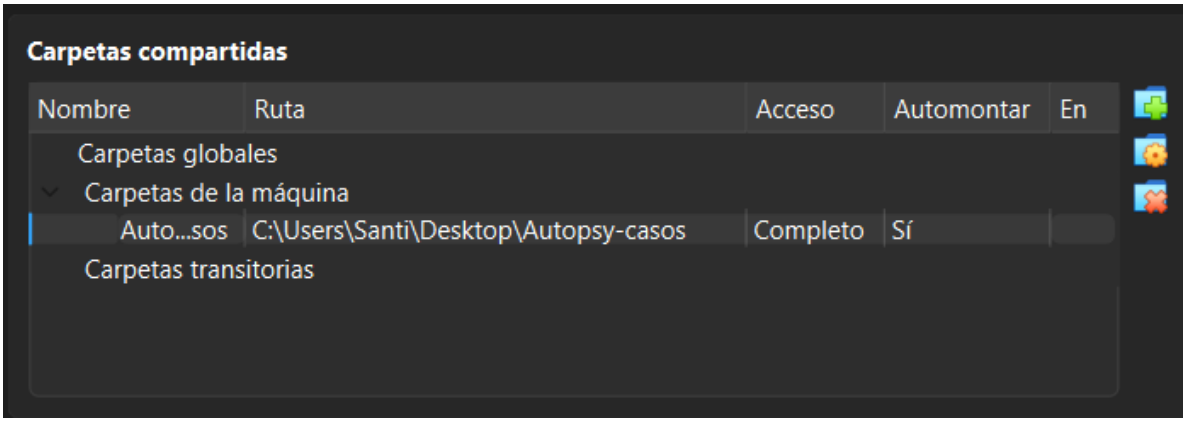


Ilustración 35 Carpetas compartidas en Kali linux

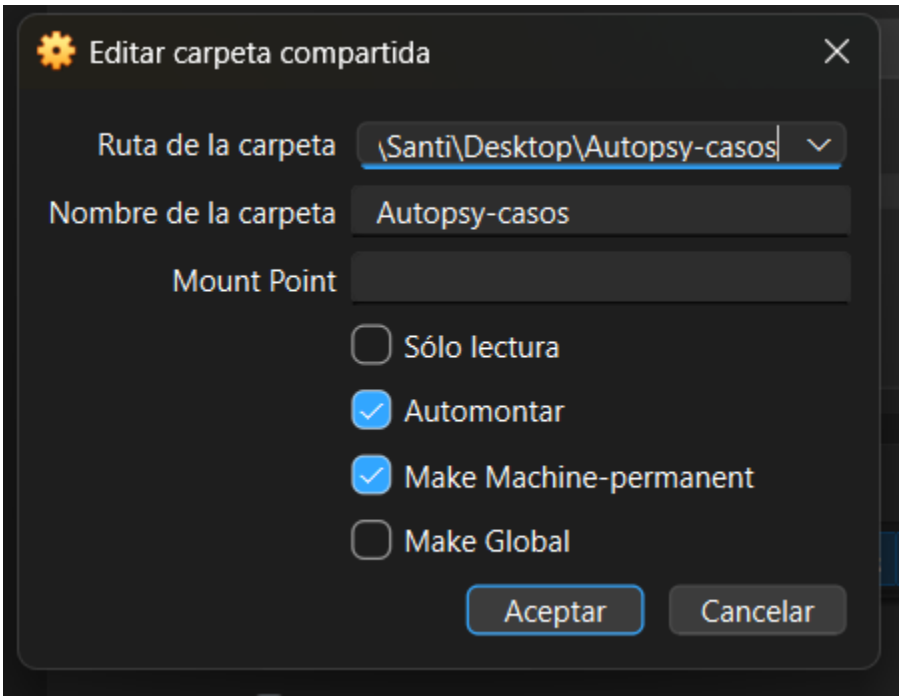


Ilustración 36 Editar carpeta compartidas (kali linux)

Autopsy permite revisar los archivos multimedia encontrados dentro de la evidencia, como fotografías o videos. Esta función ayuda a determinar si existen archivos con contenido sensible o sospechoso. El sistema puede generar vistas en miniatura y reportes con las propiedades de cada archivo. La inspección visual es un componente clave en análisis forense, pues puede revelar actividades del usuario o archivos creados fuera de los procedimientos normales del sistema operativo investigado.

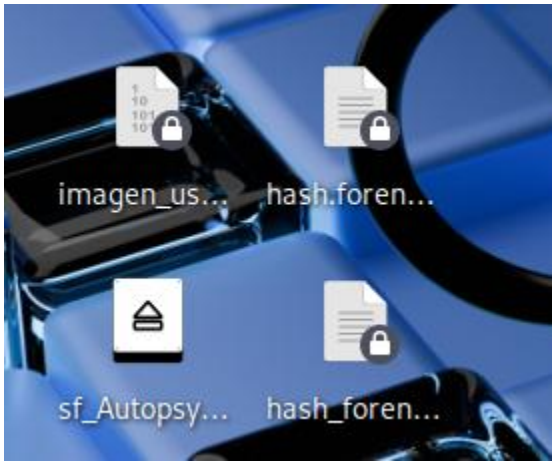


Ilustración 37 agreado del documento

En esta fase, se examinan los documentos almacenados en la memoria, incluyendo archivos de texto, Word y PDF. Autopsy permite visualizar su contenido directamente, sin necesidad de herramientas externas, para detectar posibles evidencias o información sensible. Se analizan nombres, temas o referencias relacionadas con el caso. Esta revisión documental resulta esencial, ya que los archivos de texto suelen contener registros, contraseñas o datos que aportan contexto a la investigación forense digital.

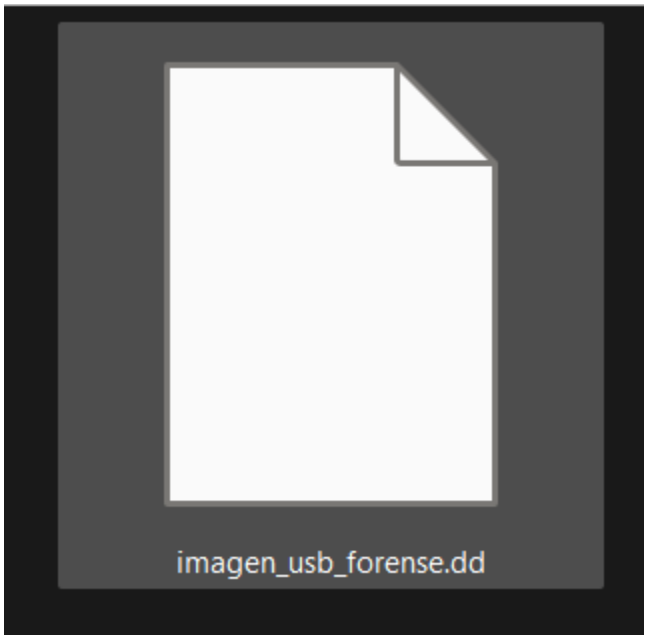


Ilustración 38 Imagen usb forense (creada)

Autopsy logra detectar archivos previamente borrados del sistema, gracias al análisis de los sectores no sobrescritos de la memoria. Estos elementos recuperados pueden incluir fotografías, registros y documentos. Se analiza su integridad y se comparan las fechas de creación y eliminación. Este tipo de recuperación es vital en investigaciones forenses, ya que permite obtener pruebas que el usuario intentó ocultar o borrar intencionalmente, manteniendo su valor probatorio dentro del análisis técnico del caso.

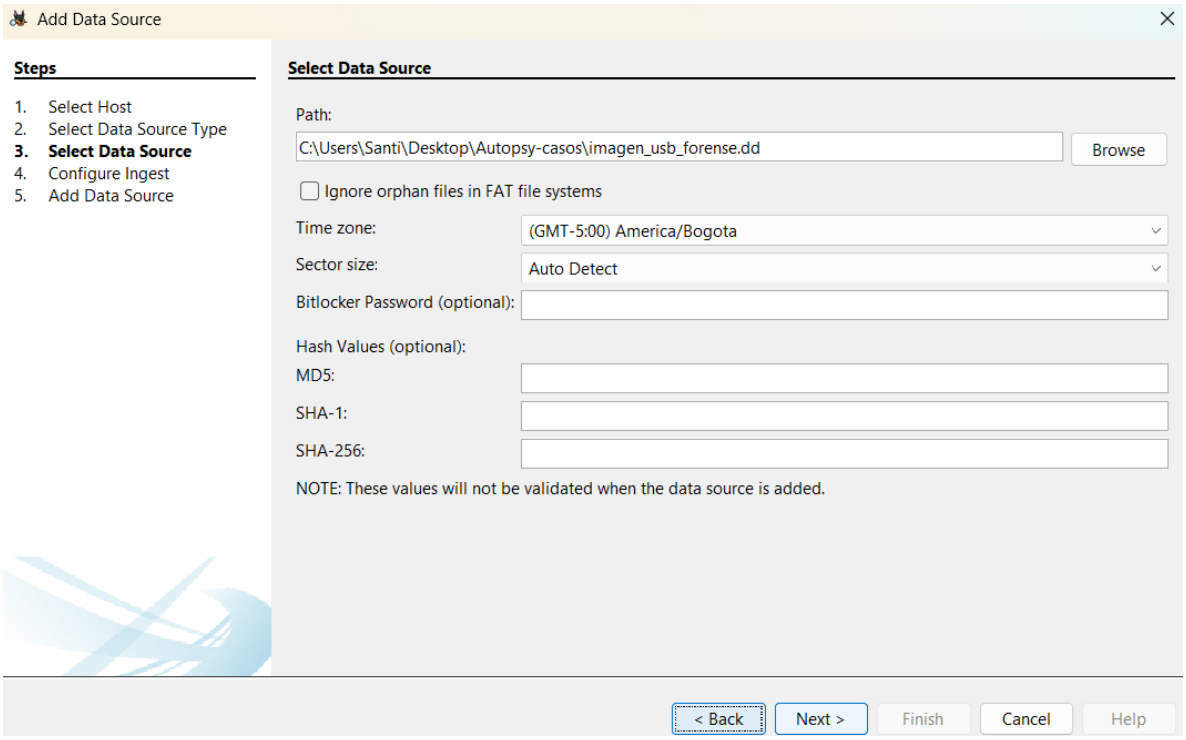


Ilustración 39 agregar fuente de datos agregar la imagen

Los artefactos del sistema, como logs, accesos recientes, archivos de registro y temporales se analizan con precisión para determinar las acciones realizadas por el usuario. Autopsy extrae información como historial de ejecución, rutas de acceso y tiempos de uso. Estos datos complementan la investigación, permitiendo al analista forense vincular eventos y actividades específicas dentro del entorno del dispositivo, contribuyendo a la obtención de evidencia sólida y cronológicamente coherente en el informe técnico final.

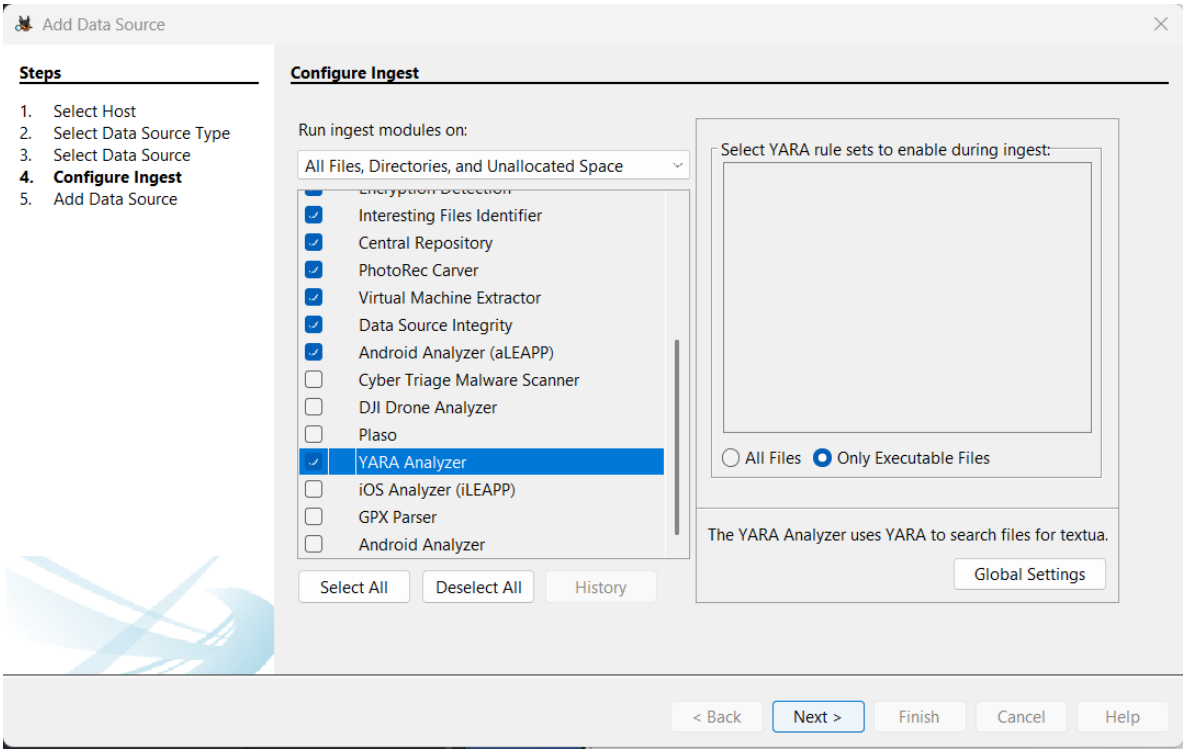


Ilustración 40 agregar fuente de datos configuracion de la ingesta

Finalizado el análisis, Autopsy permite generar un reporte automático con todos los resultados obtenidos: archivos encontrados, metadatos, palabras clave y evidencia recuperada. Este informe puede exportarse en formatos como HTML o PDF. Incluye un resumen detallado del análisis realizado y los hallazgos más relevantes. La generación del reporte fortalece la trazabilidad del proceso y permite presentar los resultados de manera clara, profesional y verificable dentro del contexto académico o pericial correspondiente.

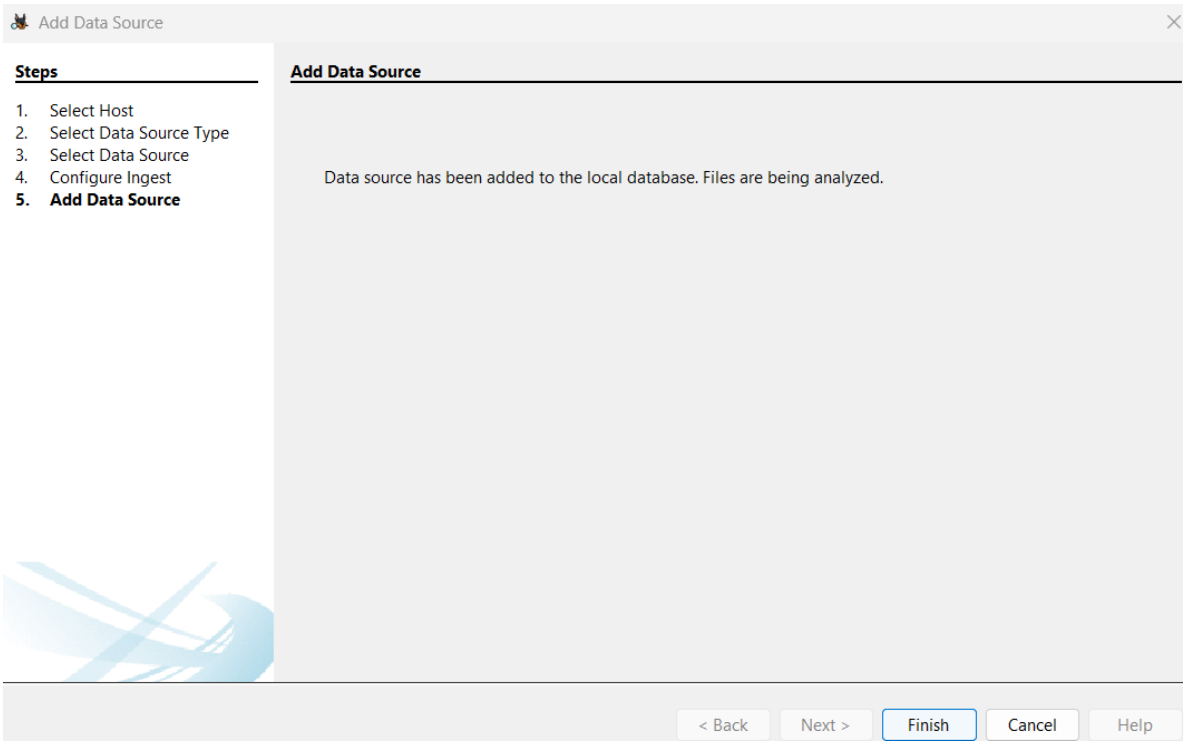


Ilustración 41 agregar fuente de datos finalizacion

generado por Autopsy se guarda en una carpeta específica, asegurando su disponibilidad para revisión o presentación. En este documento se incluyen las rutas de los archivos analizados, los resultados de búsquedas y los hashes de verificación. La exportación de los reportes permite conservar evidencia secundaria con valor probatorio. Este paso cierra la fase de análisis con Autopsy, dejando lista la documentación técnica para continuar con la validación cruzada utilizando la herramienta FTK Imager.

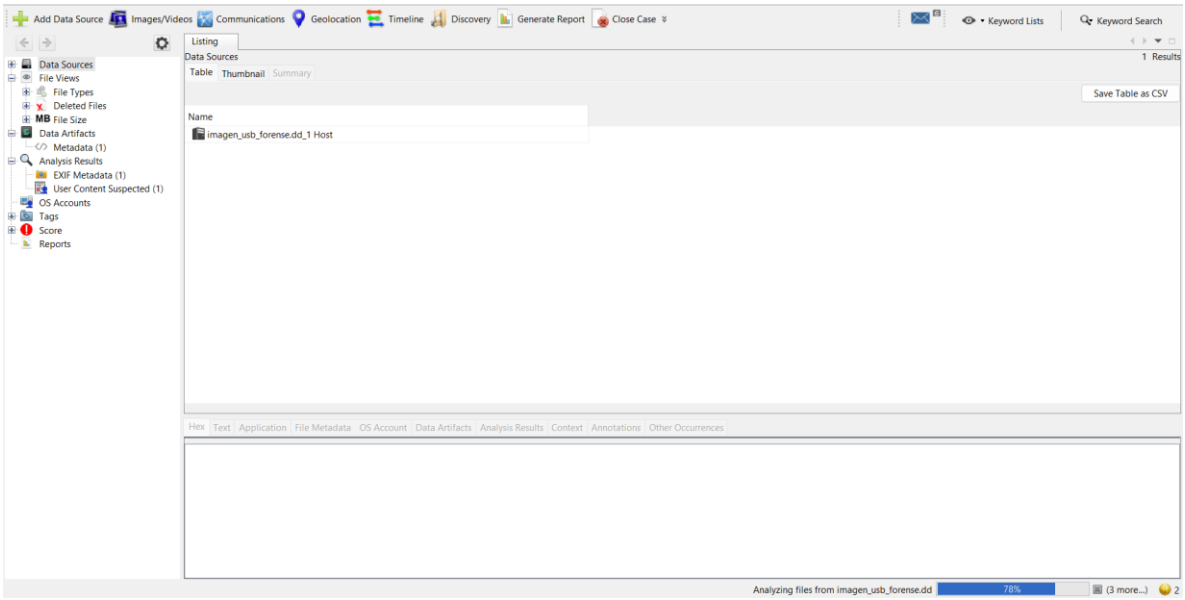


Ilustración 42 Agregacin de autposy de la imagen

El análisis y reporte finalizados, se guarda el caso en Autopsy para conservar el registro completo de la investigación. El cierre de esta fase asegura que todas las operaciones realizadas estén documentadas. Este paso marca el fin del trabajo con Autopsy y inicia la segunda etapa del análisis con FTK Imager, herramienta complementaria utilizada para verificar resultados y reforzar la validez de la evidencia digital desde otro entorno de investigación forense profesional.

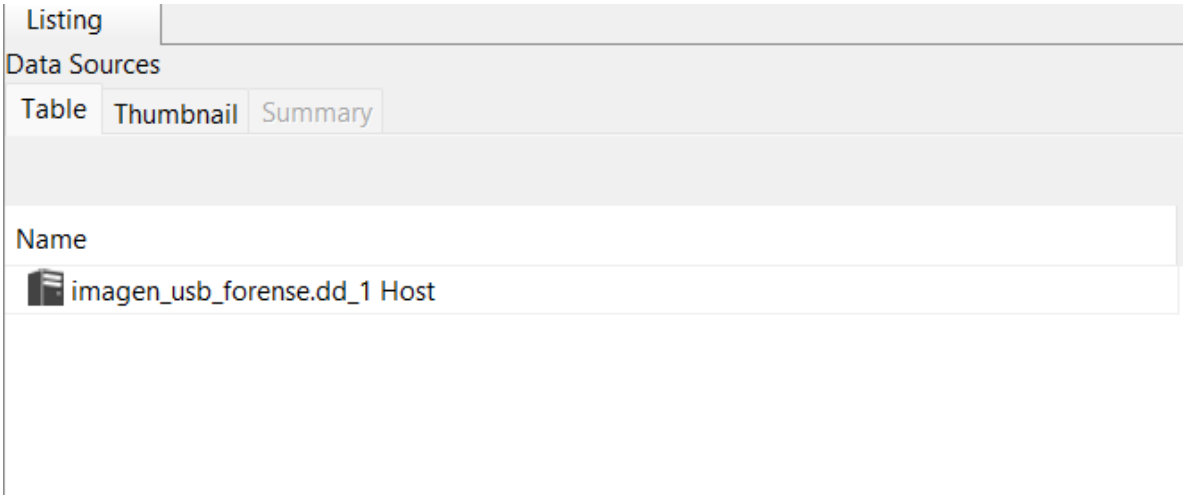


Ilustración 43 agragado de laimagen usb forense

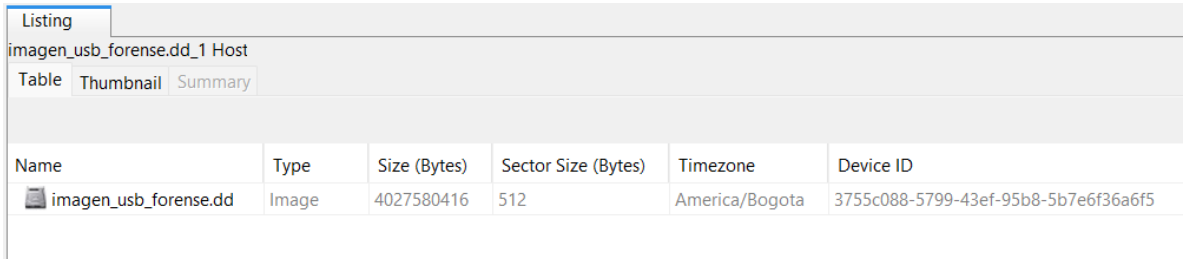


Ilustración 44 autopsy muestra los datos de la imagen usb forense

Se inicia la segunda fase del proceso utilizando el software FTK Imager en Windows. Esta herramienta se emplea para examinar, visualizar y verificar imágenes forenses. Antes de comenzar, se configura el entorno de trabajo asegurando espacio de almacenamiento y permisos administrativos. FTK Imager complementa los resultados obtenidos con Autopsy, ofreciendo una vista más directa y detallada de la estructura del sistema de archivos, garantizando la integridad de la información a lo largo del proceso forense.

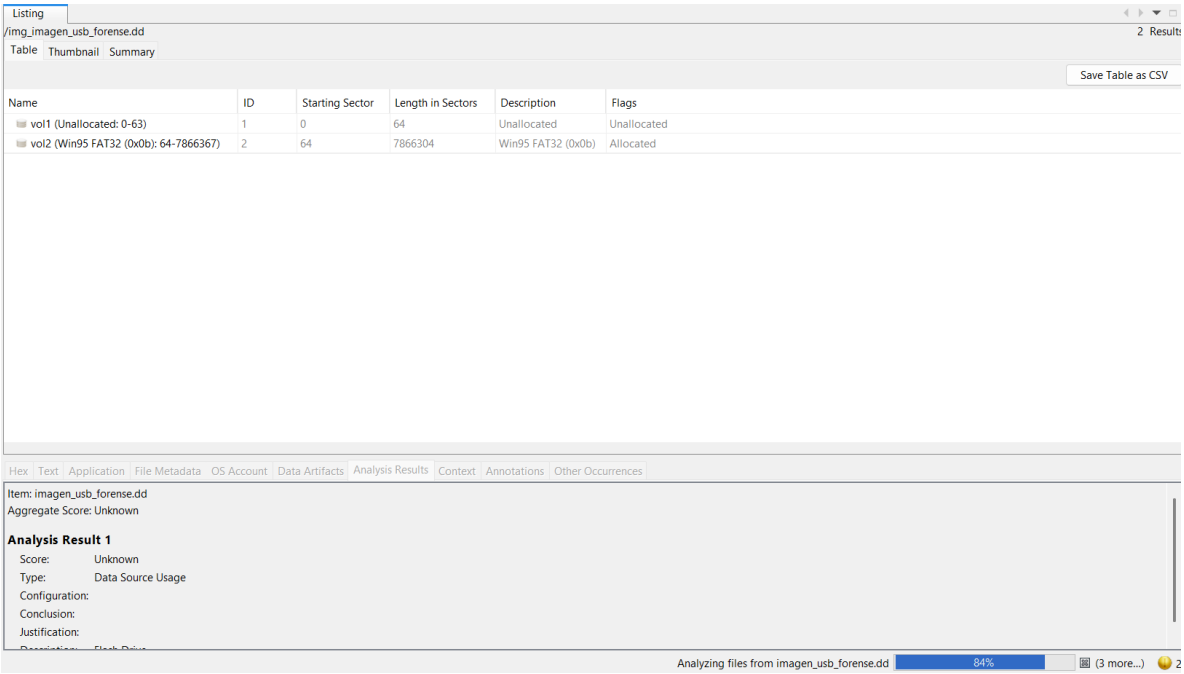


Ilustración 45 EL volumen de la imagen usb forense

Tras iniciar FTK se selecciona la opción para agregar una fuente de evidencia. Esta imagen muestra la ventana donde el analista debe especificar el tipo de evidencia a cargar. En este caso, se seleccionará la opción **"Image File"** para importar la imagen forense previamente creada (**imagen_usb_forense.dd**), este paso es crucial, ya que se establece la conexión entre la herramienta de verificación (FTK Imager) y la copia bit-a-bit de la evidencia original, preparándola para su exploración sin alterar el archivo fuente

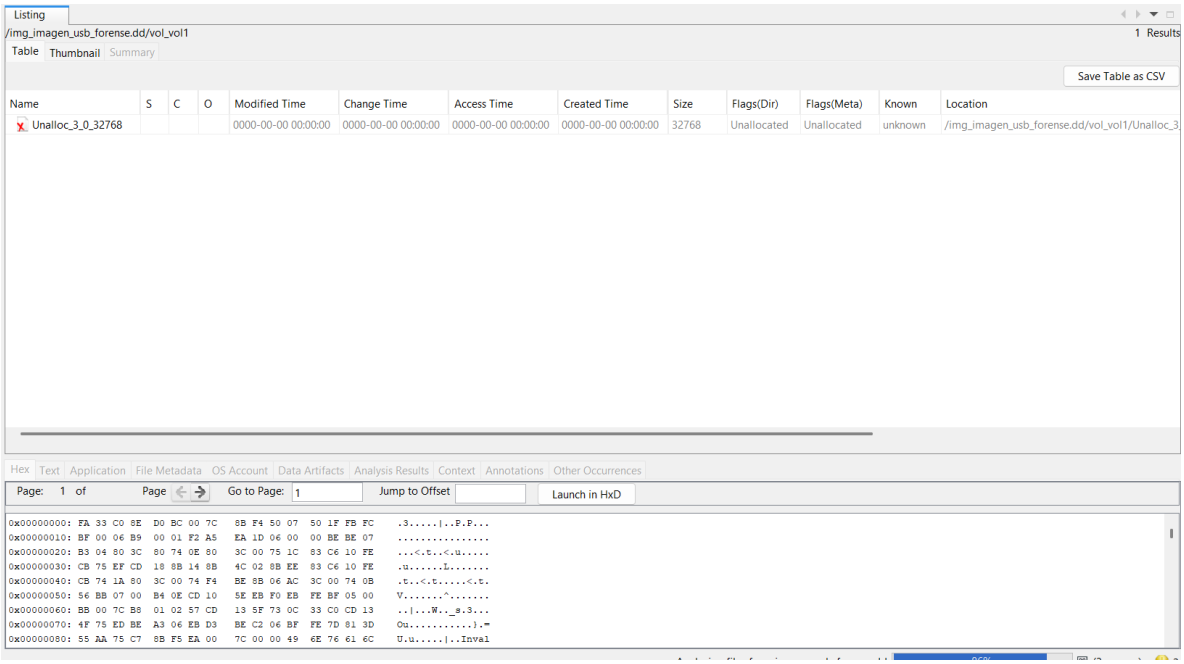


Ilustración 46 Muestra de los datos de la imagen usb forense

Una vez que la imagen forense ha sido cargada, esta imagen muestra la estructura de archivos que FTK Imager ha interpretado. Se puede observar el árbol de directorios lógicos de la partición, lo que permite al analista navegar por las carpetas del dispositivo tal como estaba en el medio original. Esta exploración es fundamental para **confirmar la coherencia** de la estructura de archivos con los resultados obtenidos previamente en Autopsy. La vista en árbol es un punto clave para la verificación cruzada, asegurando que los directorios y archivos estén completos y utilizables en ambas herramientas.

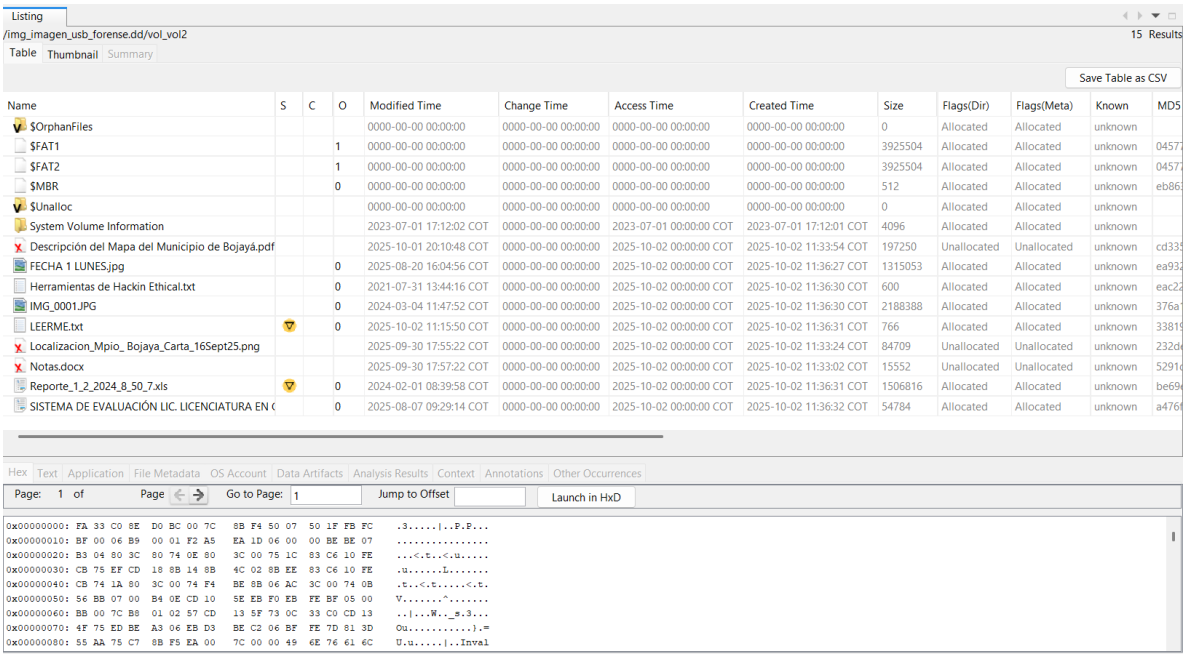


Ilustración 47 Exploración del contenido de la imagen en FTK Imager.

Esta imagen documenta el análisis individual de un archivo dentro de FTK Imager. Se selecciona un elemento del árbol y el panel de detalle a la derecha muestra las propiedades del archivo, incluyendo su nombre, ruta, y, lo más importante, su valor **MD5 y/o SHA1 hash** calculado por FTK Imager. Este procedimiento permite **comparar de forma inmediata** los hashes de los archivos específicos con los encontrados en Autopsy, reforzando la verificación cruzada. Además, esta vista prepara el camino para la inspección más profunda a nivel hexadecimal, crucial para detectar rastros de manipulación

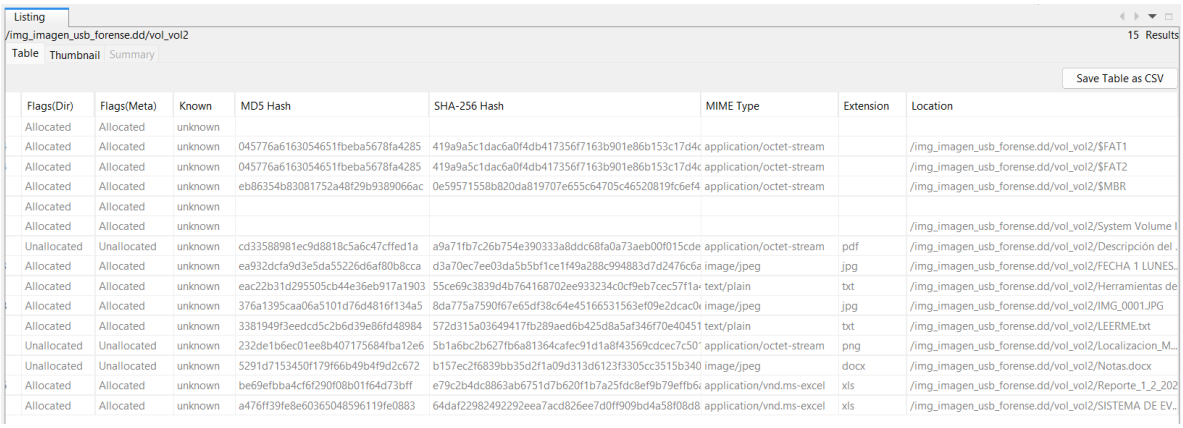


Ilustración 48 Análisis de propiedades de archivo y cálculo de hash en FTK Imager.

8 ANÁLISIS FORENSE DE EVIDENCIAS DIGITALES CON FTK IMAGER EN WINDOWS.

8.1 INSTALACION DE FTK IMAGER

En esta etapa se realiza la búsqueda del instalador oficial de **FTK Imager** versión 4.7.3.81 desde el portal de **Exterro**, desarrollador actual del software. Se accede al enlace oficial (www.exterro.com/ftk-imager) para garantizar la obtención de una versión segura y actualizada del programa.

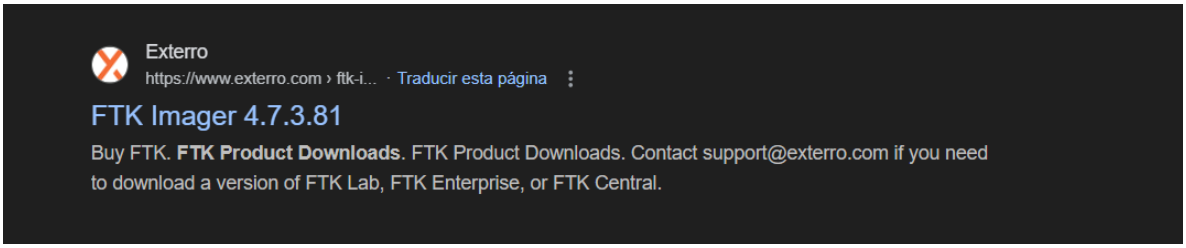


Ilustración 49 Pagina web de FTK IMAGER

Paso al siguiente, se visualiza el apartado **"Product Downloads"** del sitio oficial de Exterro, donde se encuentra disponible la versión **FTK Imager 4.7.3.81**. Desde este enlace se descarga el instalador del software utilizado para realizar análisis forenses digitales en entornos Windows.

Ilustración 50 instalacion del programa de FTK IMAGER

8.2 DILIGENCIAMIENTO DEL FORMAULARIO DE DESCARGA DE FTK IMAGER PRO-8.2

En esta imagen se muestra el proceso realizado para la **descarga oficial del software FTK Imager Pro-8.2** desde la página web de **Exterro**. En este paso, el estudiante **Santiago Quinto Copete** completa el formulario de registro requerido por la plataforma, ingresando los datos personales y académicos solicitados:

- **Nombre:** Santiago
- **Apellido:** Quinto Copete
- **Correo electrónico:** santiagocopete15@gmail.com
- **Nombre de la organización:** Utch–PITI
- **Título profesional:** Auditorio profesionalismo
- **País:** Colombia

El llenado correcto de este formulario permite acceder al enlace de descarga legítimo y verificar la procedencia del software. Este procedimiento garantiza que la herramienta se obtenga directamente desde el sitio oficial, cumpliendo con los protocolos de seguridad y autenticidad necesarios en el ámbito forense digital.

Ilustración 51 Creacion los datos personales

8.3 PAGINA DE OFICIAL DE EXTERRO PARA LA DESCARGA DE FTK

En la interfaz se destaca la sección **“Create Forensic Images with Exterro FTK Imager”**, donde se explica que esta aplicación es utilizada globalmente por profesionales forenses para capturar, visualizar y verificar datos digitales. Desde este punto, se selecciona la opción **“Free Download”**, la cual permite iniciar el proceso de descarga segura del instalador más reciente de FTK Imager.

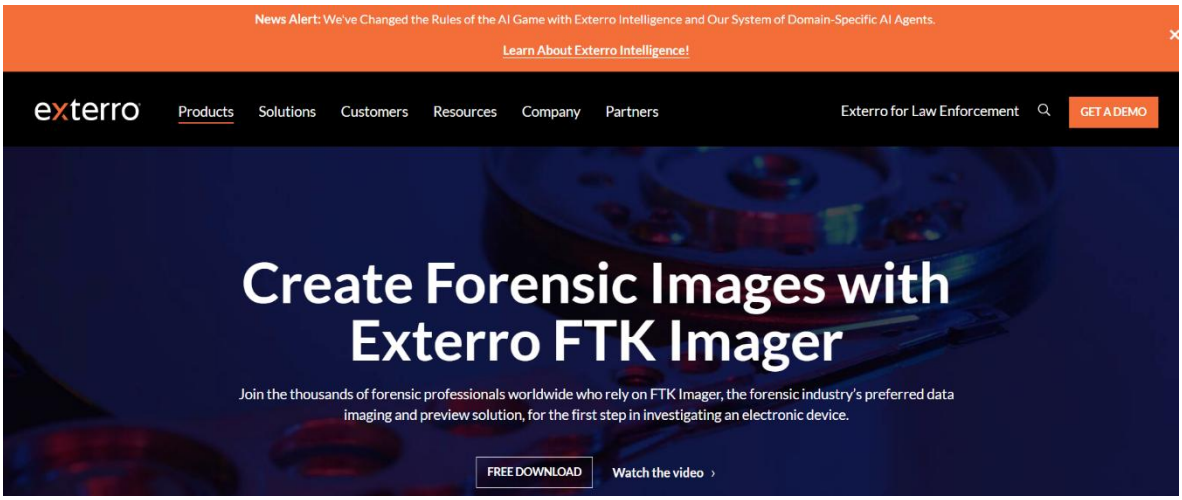


Ilustración 52 la página web de la instalación de FTK IMAGER

8.4 GUIA EXTERNA SOBRE LA INSTALACION DE FTK IMAGER EN WINDOWS

En esta imagen se presenta el sitio web **Tecno Sender**, donde se encuentra una guía detallada titulada **Cómo instalar FTK Imager en Windows**, Esta fuente ofrece una explicación paso a paso para realizar la descarga, instalación y configuración inicial de la herramienta forense. En esta etapa, el estudiante **Santiago Quinto Copete** consulta la guía como apoyo técnico para confirmar los procedimientos correctos antes de ejecutar la instalación.

La página muestra los **requisitos previos**, entre ellos: disponer de un equipo con **Windows 10 o superior**, contar con conexión a Internet estable y tener **permisos de administrador** para instalar el programa. Posteriormente, se describe el **Paso 1: Descargar FTK Imager**, incluyendo el enlace oficial hacia el sitio de **Exterro (AccessData)**, donde se encuentra la versión legítima del software.

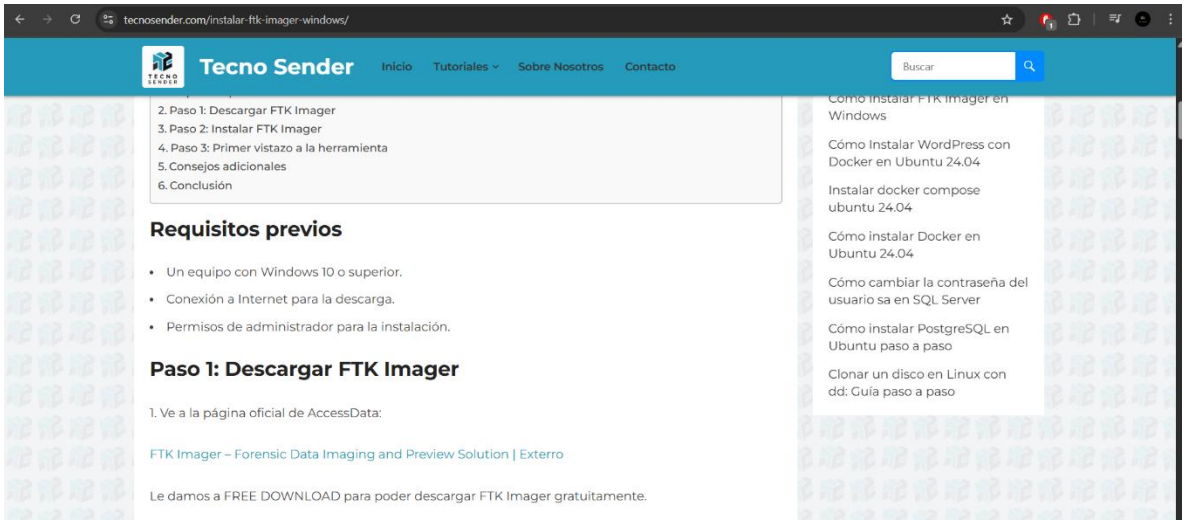


Ilustración 53 la pagina de Tecno sender para descargar

8.5 REGISTRO PARA DESCARGA OFICIAL DE FTK IMAGER 4.7.

En esta imagen se observa el formulario de registro oficial de **Exterro** para la descarga del software **FTK Imager versión 4.7**, herramienta empleada en el análisis forense digital. El formulario solicita información básica del usuario, incluyendo nombre, correo institucional, organización, cargo y país. En este caso, los datos ingresados corresponden al estudiante **Santiago Quinto Copete**, perteneciente a la institución **UTCH** (Universidad Tecnológica del Chocó) y al área de **Seguridad y Auditoría de Redes – PITI**.

La interfaz describe brevemente las funciones principales de FTK Imager, como la **creación de imágenes forenses de discos locales y memorias USB**, la **visualización del contenido de dichas imágenes**, y la **generación de valores hash** mediante

los algoritmos **MD5** o **SHA-1** para verificar la integridad de la evidencia digital.

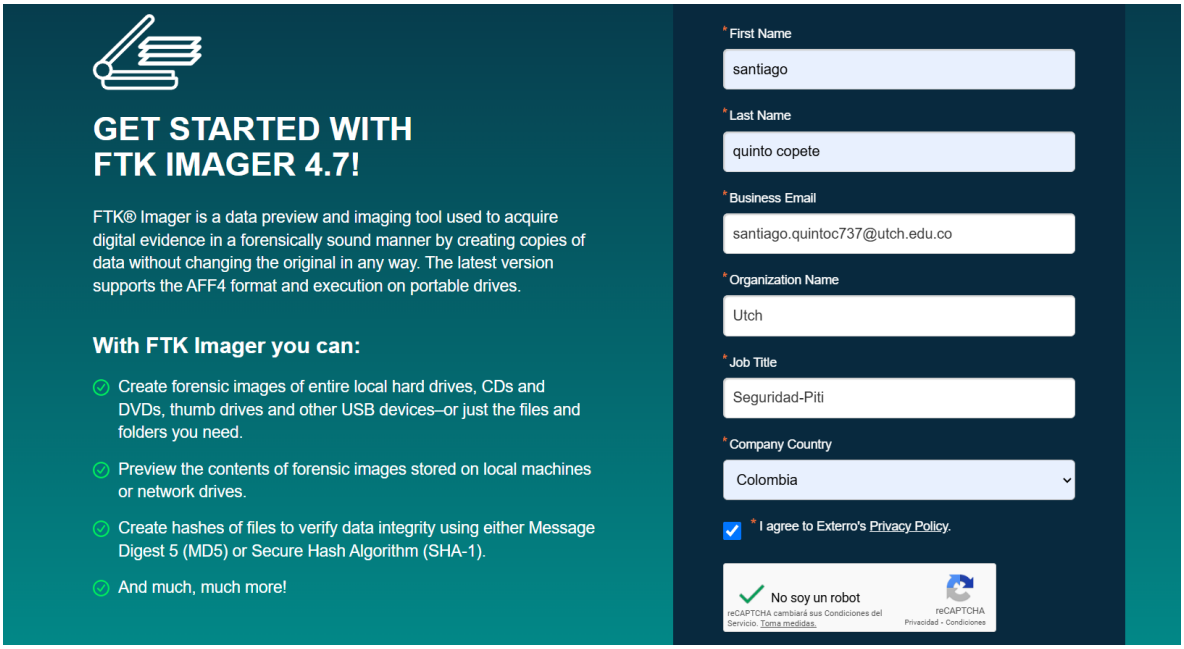


Ilustración 54 Creacion de datos personal

Luego se abrió en una notificación de las descargas, se está instalando de la **FTK imager**

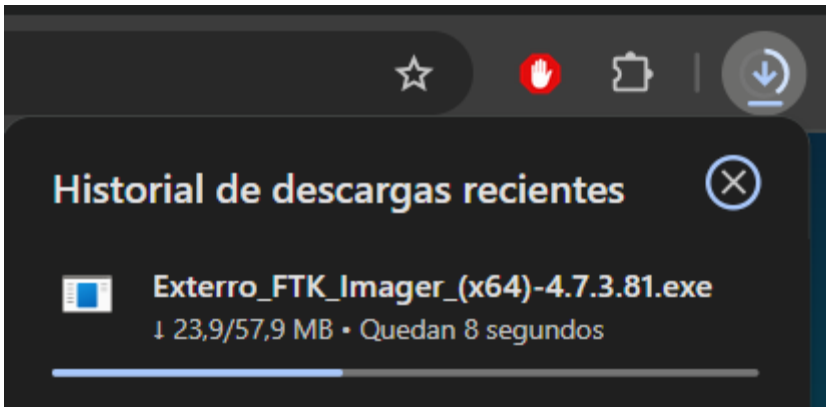


Ilustración 55 Descargando de FTK IMAGER

Se instalo correctamente de la aplicación de **FTK IMAGER**

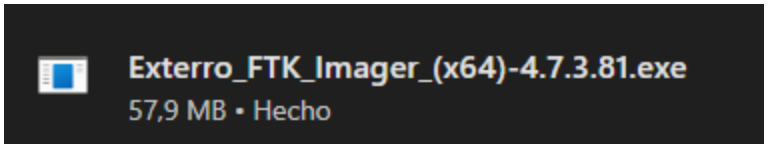


Ilustración 56 instalado completamente

8.6 PROGRAMA DE FTK IMAGER

Luego de eso, en app está en la carpeta de la descarga, luego le daremos clic

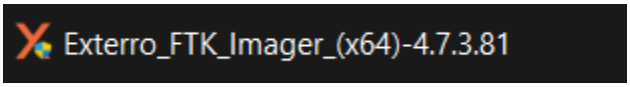


Ilustración 57 el programa está instalado en la descarga

Veamos en el siguiente paso, se abrió en el programa de **FTK IMAGER**, se esta corriendo para poder empezar con el proceso de lo que debe hacer

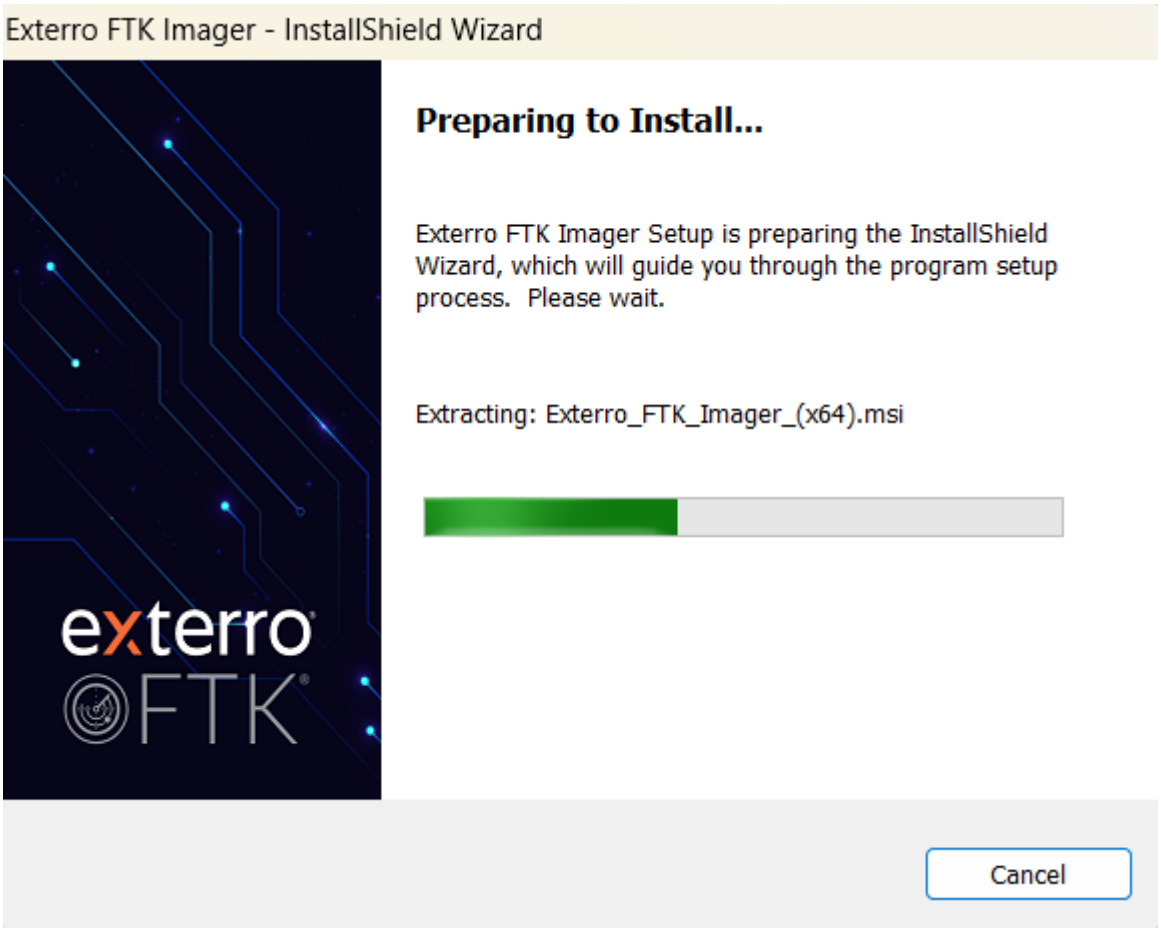


Ilustración 58 Preparando para instalar

Veamos el siguiente paso, le esta dando bienvenida en nuestra app, para poder desarrollar en FTK IMAGER, luego daremos clic donde dice **NEXT.**

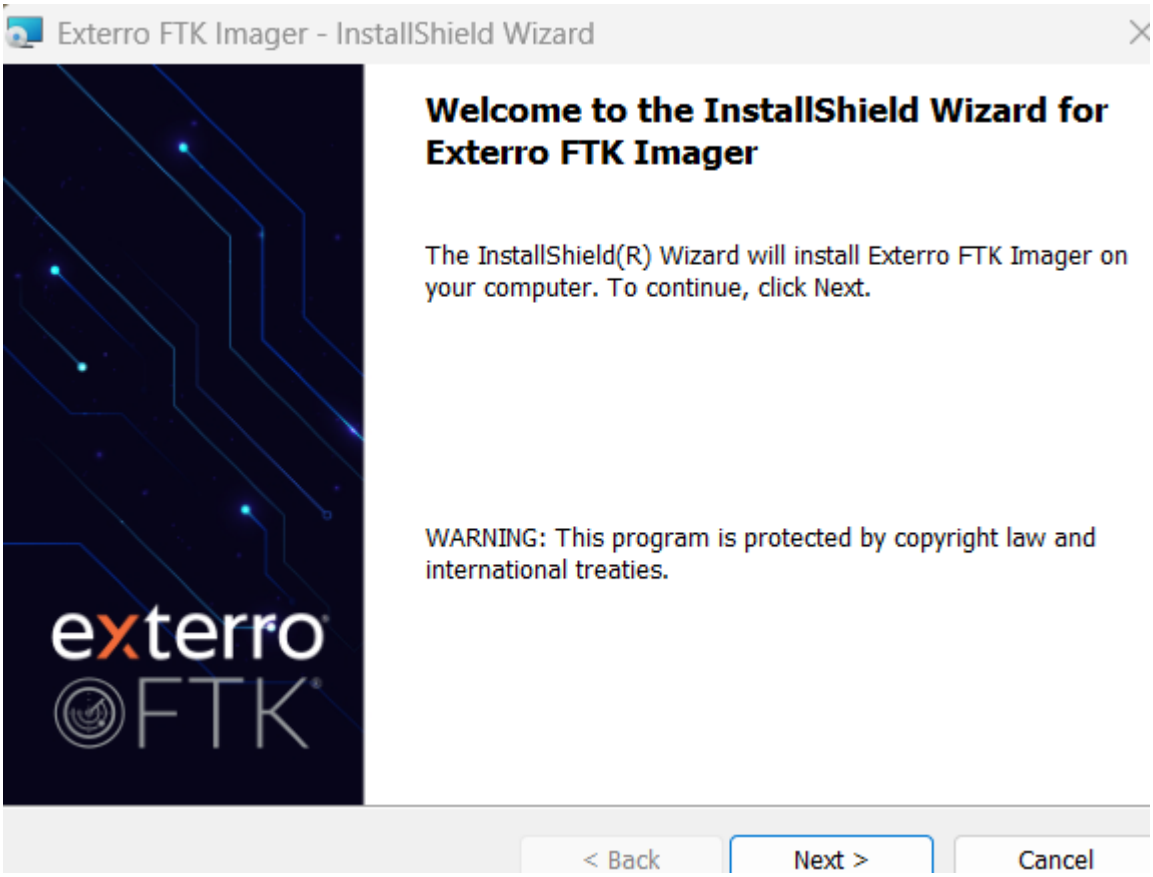


Ilustración 59 Exterro FTK Imager - Asistente de instalación

8.7 ACUERDO LICENCIDA DE USUARIO FINAL PARA EXTERRO

Veamos el siguiente paso, esto es una licencia de usuario, luego le daremos en la opción donde dice **aceptar los términos del acuerdo de licencia**, luego le daremos de nuevamente para el siguiente paso **NEXT**

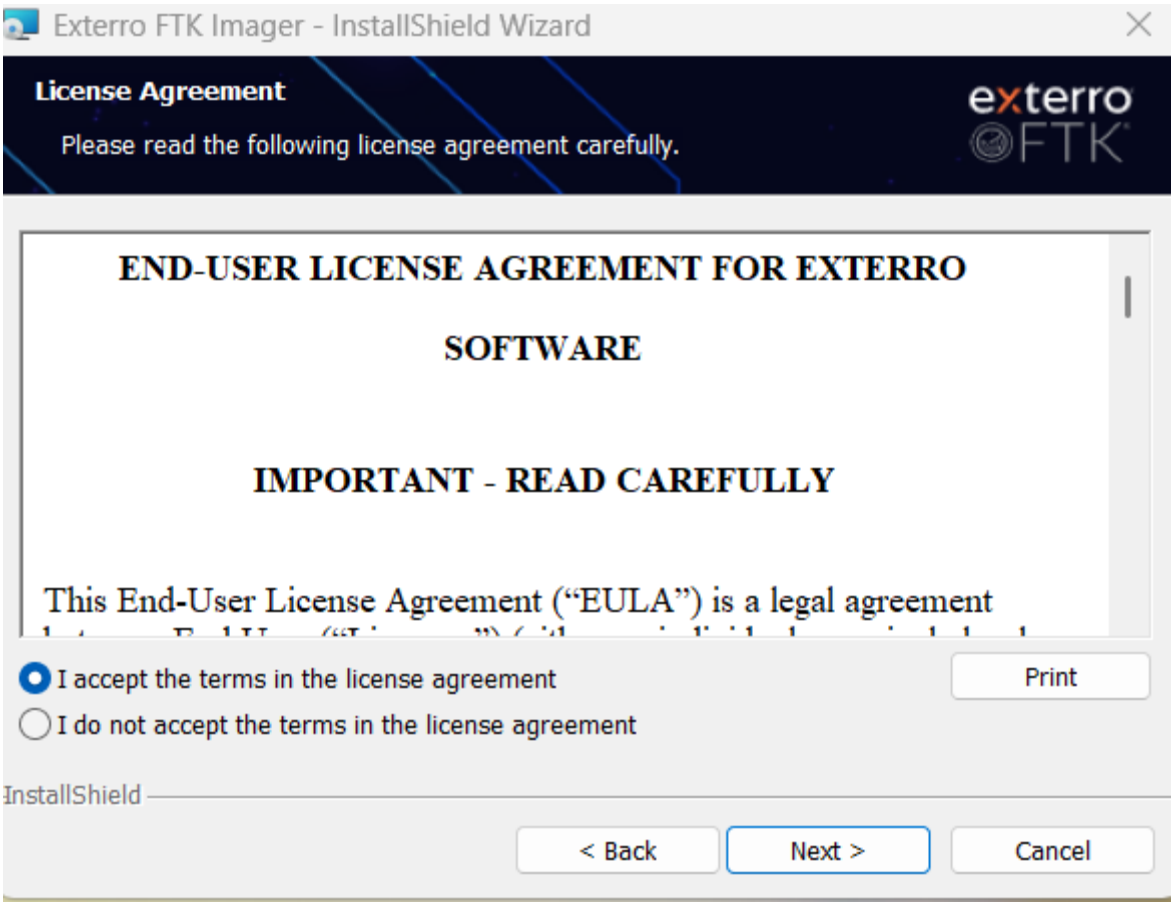


Ilustración 60 Acuerdo de licencia

8.8 CARPETA DESTINO

Veamos el siguiente paso, una vez que eso se va guardar en el destino en el programa de archivos, ahí dice que se va a agregar en la ruta de instalación en oa lista de exclusiones de Windows defender, luego les daremos en el siguiente paso **NEXT.**

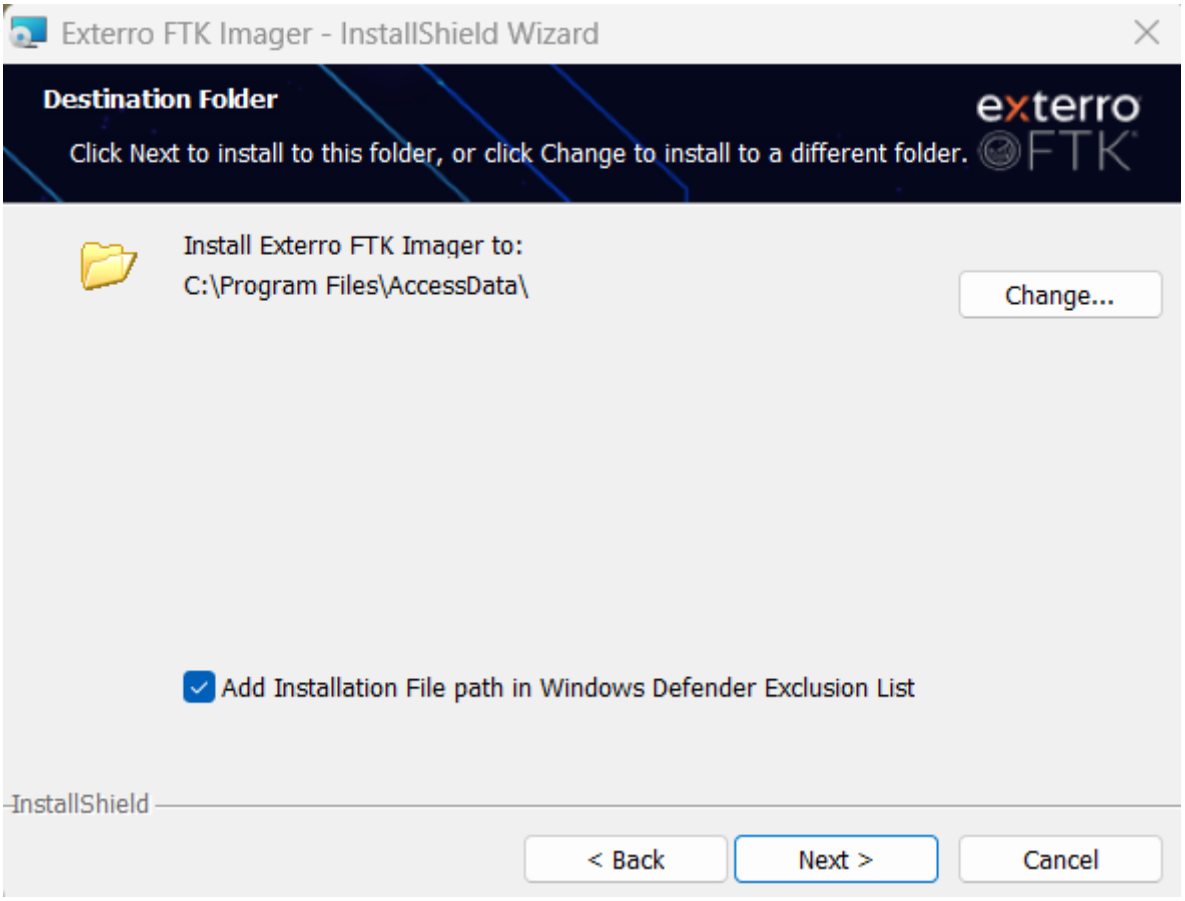


Ilustración 61 carpeta de destino

8.9 INSTALAR EN EL PROGRAMA DE FTK IMAGER

Veamos el siguiente paso, para poder empezar de la instalación del programa para empezar instalación, luego les daremos clic **install** (instalar).

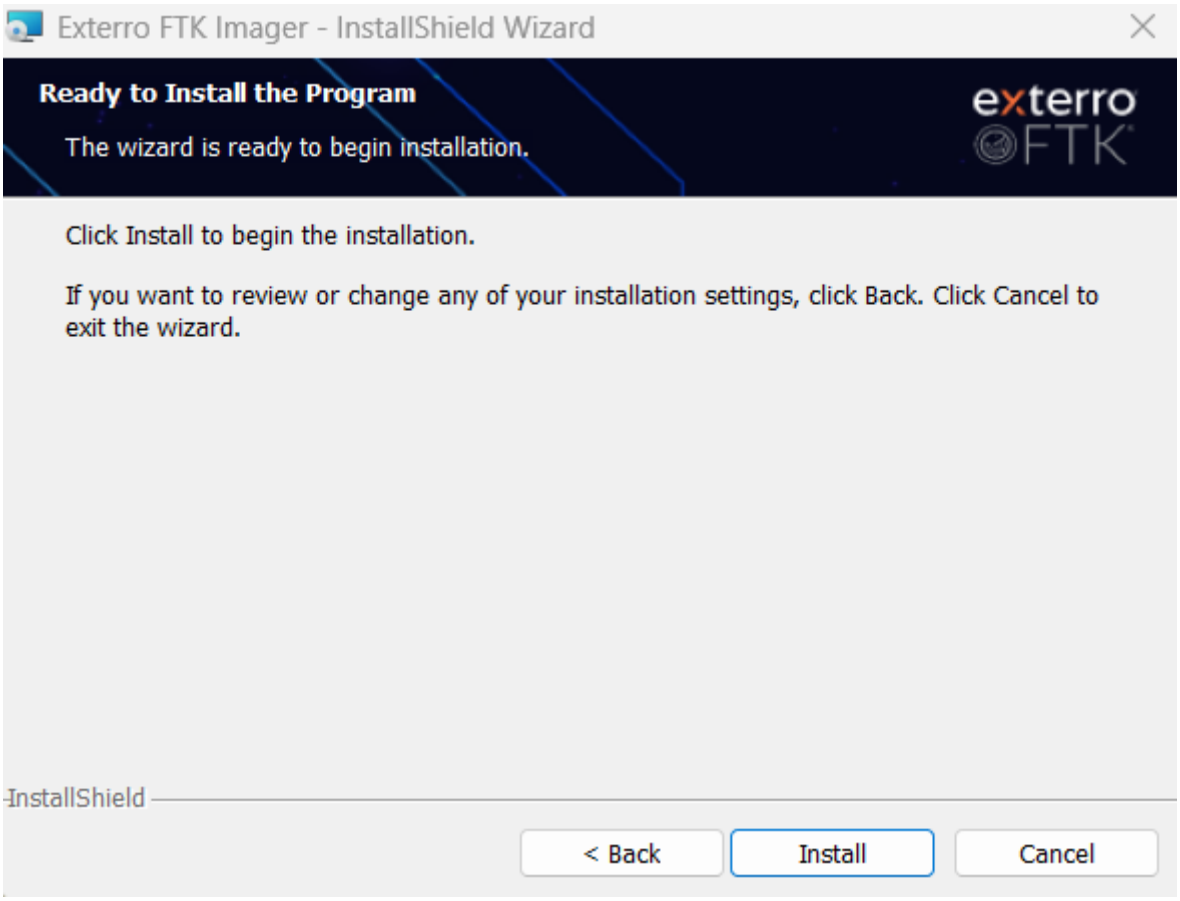


Ilustración 62 Listo para instalar el programa

8.10 INSTALANDO DE PROGRAMA DE FTK IMAGER

se está instalando en el programa de FTK IMAGER, y esperar que instale correctamente.

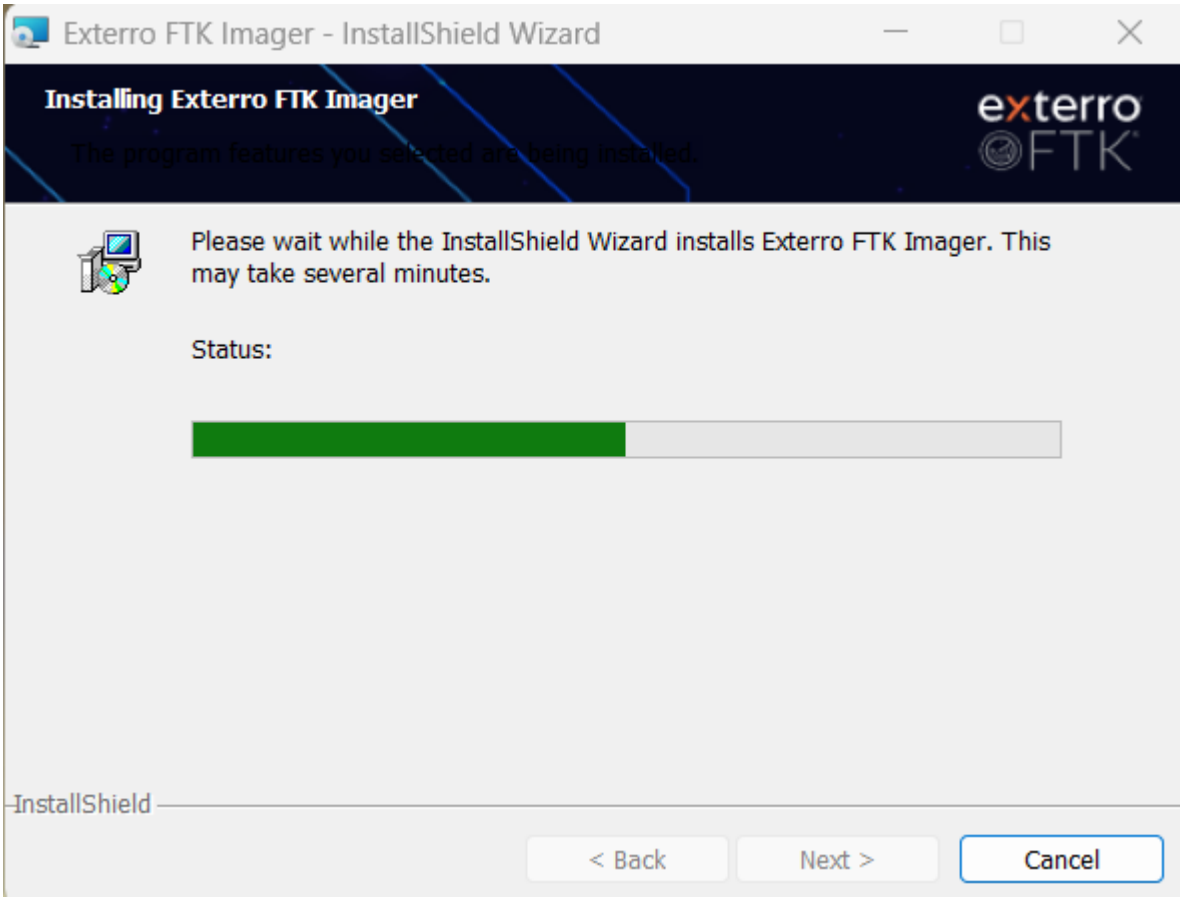


Ilustración 63 Corriendo de programa

al finalmente que ya se instaló correctamente de programa de FTK IMAGER, la opción se de iniciar EXTERRO FTK IMAGER luego les daremos clic **FINSH.**

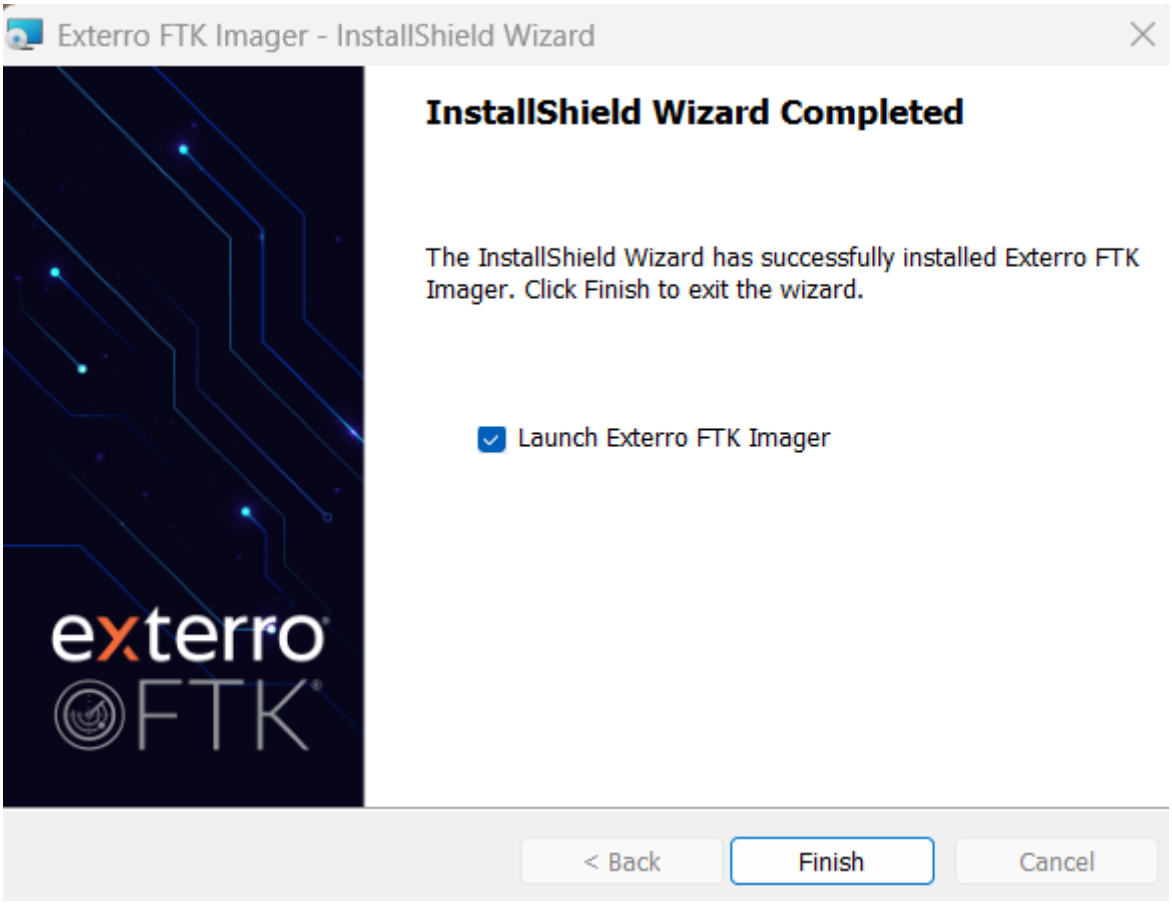


Ilustración 64 Finalizacion de la instalacion del programa de FTK IMAGER

8.11 EJECUCION DE FTK DE IMAGER

Luego veamos el siguiente paso, se abrió el programa de **FTK IMAGER.**

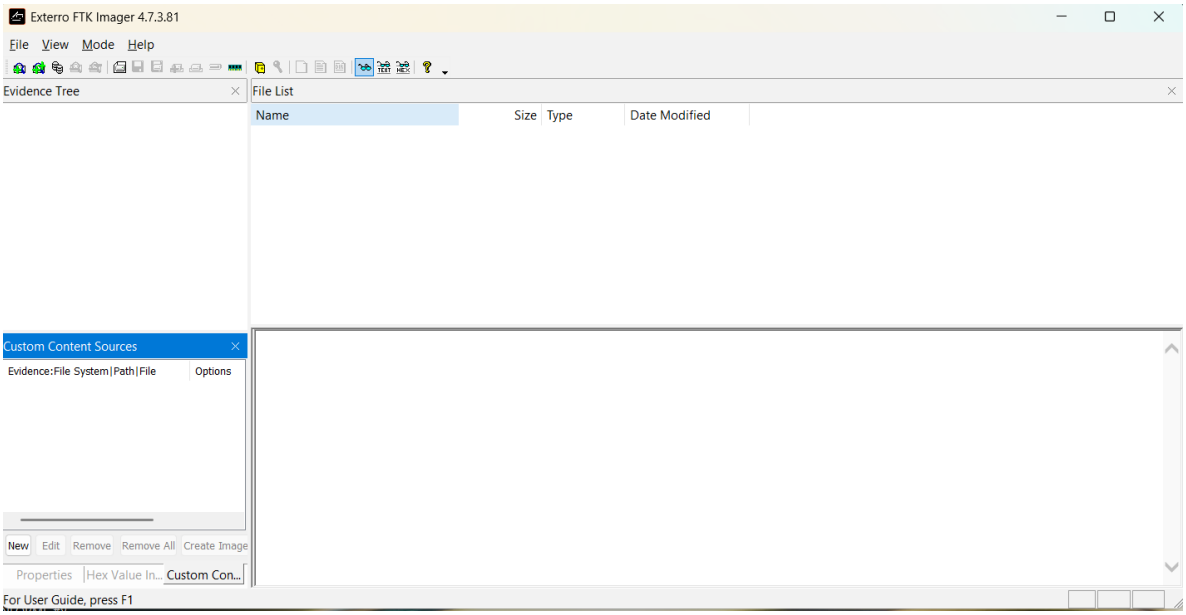


Ilustración 65 Principal de FTK IMAGER

Veamos el siguiente paso de lo que vamos a hacer, vamos a dar en clic para agregar elemento de evidencia la que tiene el signo **"+"**, es para agregar en una **imagen_usb_forense.dd.**

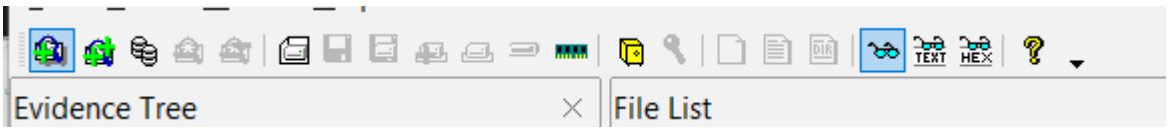


Ilustración 66 Agreacionn de un archivo

8.12 SELECCIONAR FUENTE

Se abrió para agregar de la selección con el tipo de evidencia de la fuente, lo primero que debemos seleccionar es **physcal drive** (unidad fisica) y luego le daremos clic al siguiente paso **Next** (siguiente).

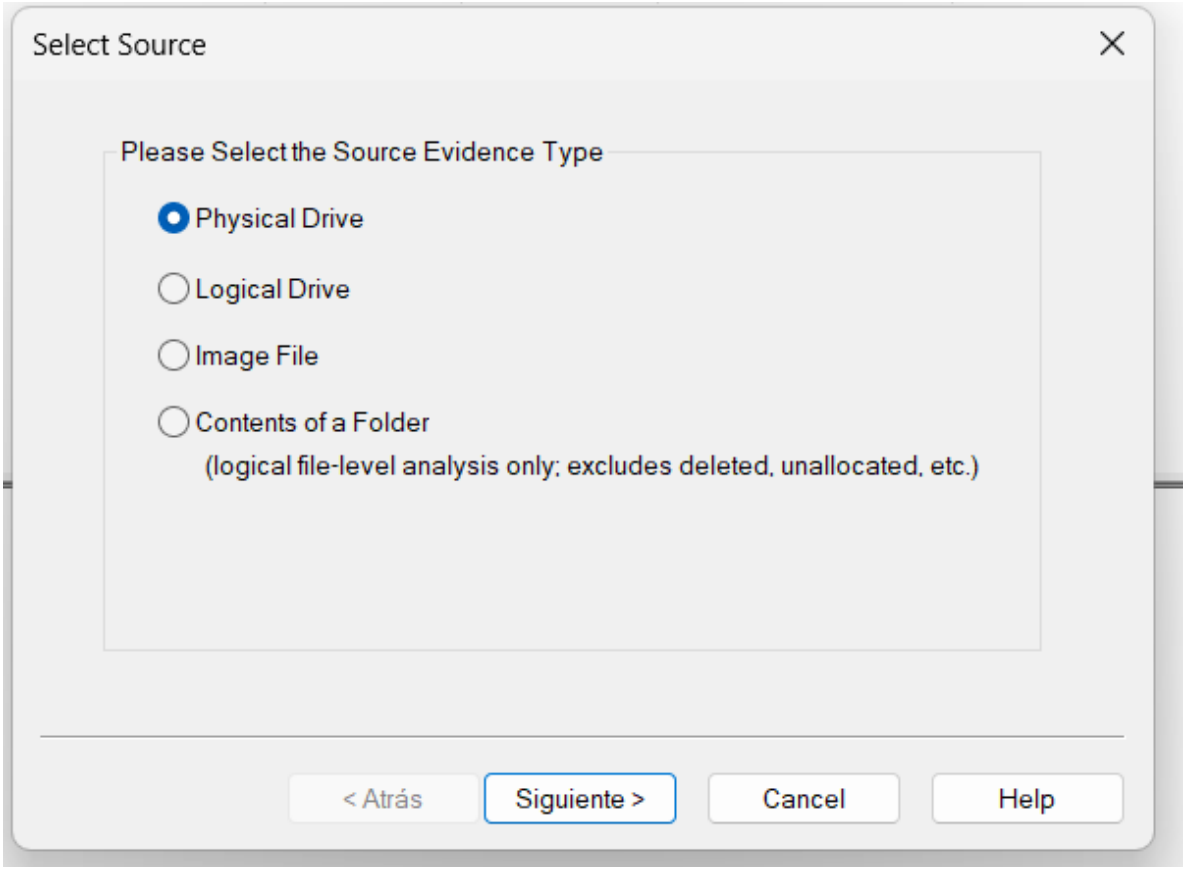


Ilustración 67 seleccionar fuerza

8.13 SELECCIONAR ARCHIVO

Veamos en el siguiente paso, lo primero que todo que tenemos que escribir de la ruta que escribimos en la ruta de la **imagen_usb_forense.dd,** le escribiremos de la ruta completamente o copiar, la ruta es **C:\Users\Santi\Desktop\Autopsy-casos\imagen_usb_forense.dd,** luego les daremos en clic **finish** (finalizado)

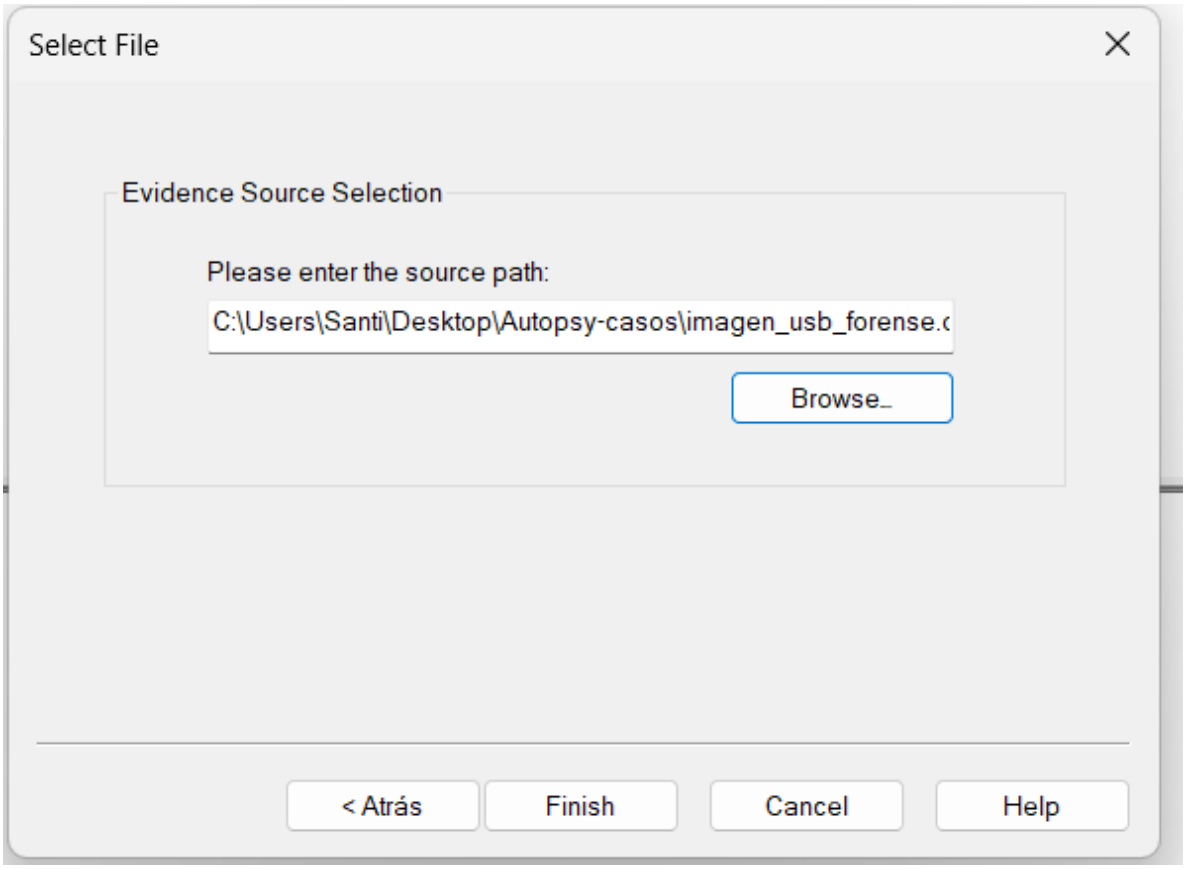


Ilustración 68 Seleccionar archivo

Veamos el siguiente paso, se muestra el software Forensic Toolkit (FTK) Imager abierto, cargando una imagen forense llamada **"imagen_usb_forense.dd"**. Se visualiza la estructura de particiones y datos hexadecimales para análisis forense digital de un dispositivo USB.

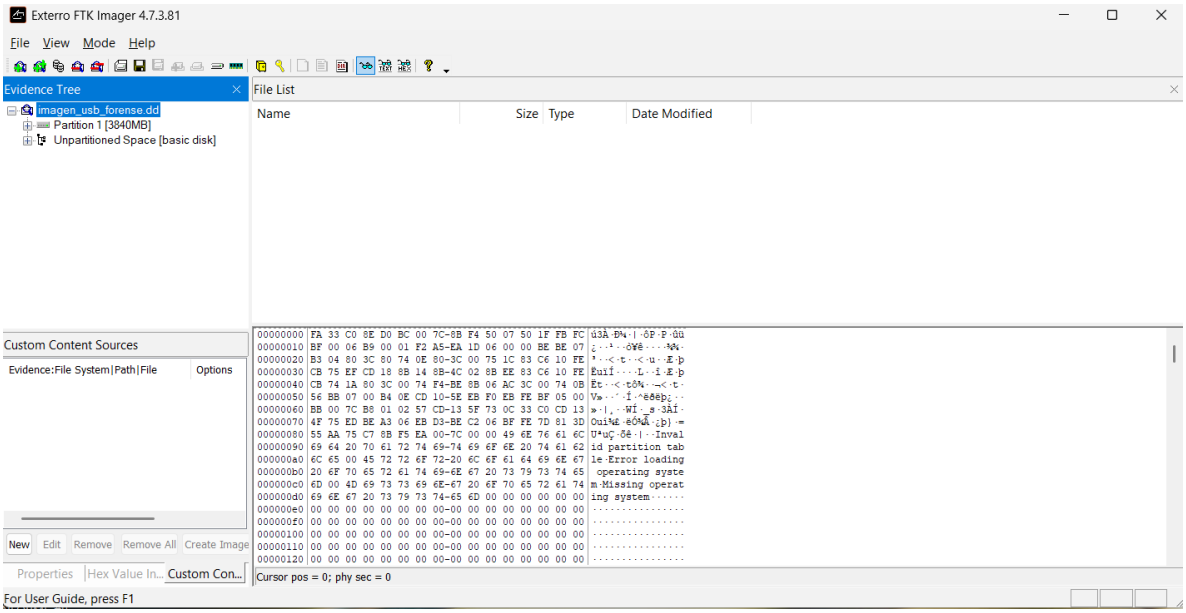


Ilustración 69 Muestra de los datos en FTK IMAGER

Observe esta imagen se muestra la herramienta Forensic Toolkit (FTK) Imager explorando el contenido de una imagen forense llamada "**imagen_usb_forense.dd**". En el panel izquierdo se observa la estructura de archivos dentro de la partición FAT32 llamada "**NONAME**". En el panel central están listados los archivos y carpetas, incluyendo imágenes JPG, archivos de texto y archivos de sistema. En la parte inferior derecha se muestra una vista en hexadecimal de los datos del archivo seleccionado,

lo que permite un análisis profundo a nivel byte para investigaciones forenses digitales.

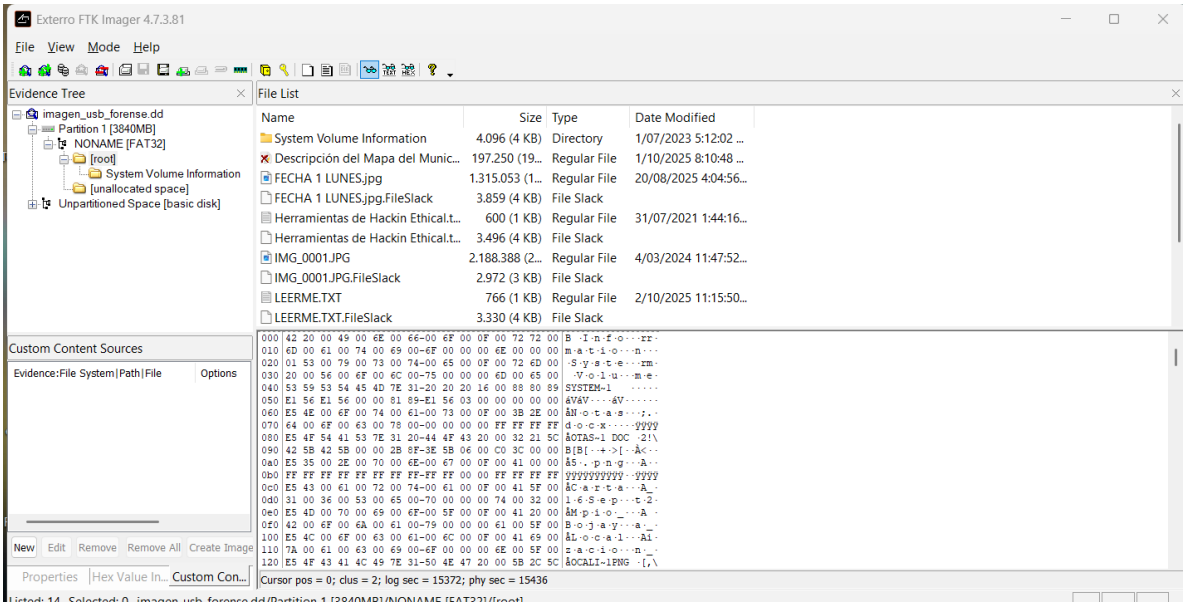


Ilustración 70 Muestra de los archivos y datos

Observe esta imagen, se analizó la imagen forense de una unidad USB en FTK Imager, identificando archivos activos y datos en file slack, destacan documentos, imágenes y archivos residuales, algunos con fechas recientes, el análisis hexadecimal revela posibles restos de información eliminada, útil para investigación digital forense.

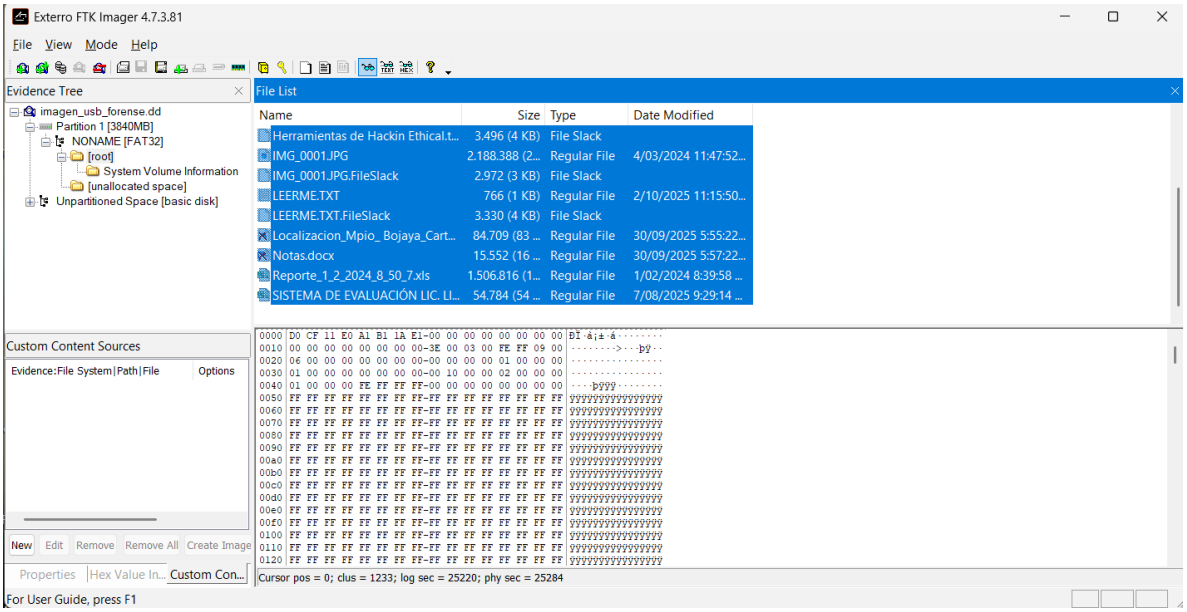


Ilustración 71 Seleccionador de los archivos

En esta imagen se observa el proceso de guardado de un archivo **.csv** con el nombre **santiago quinto** en la carpeta **Autopsy-casos**. Esto indica que se está exportando información forense posiblemente relacionada con un análisis previo realizado en FTK Imager u otra herramienta similar.

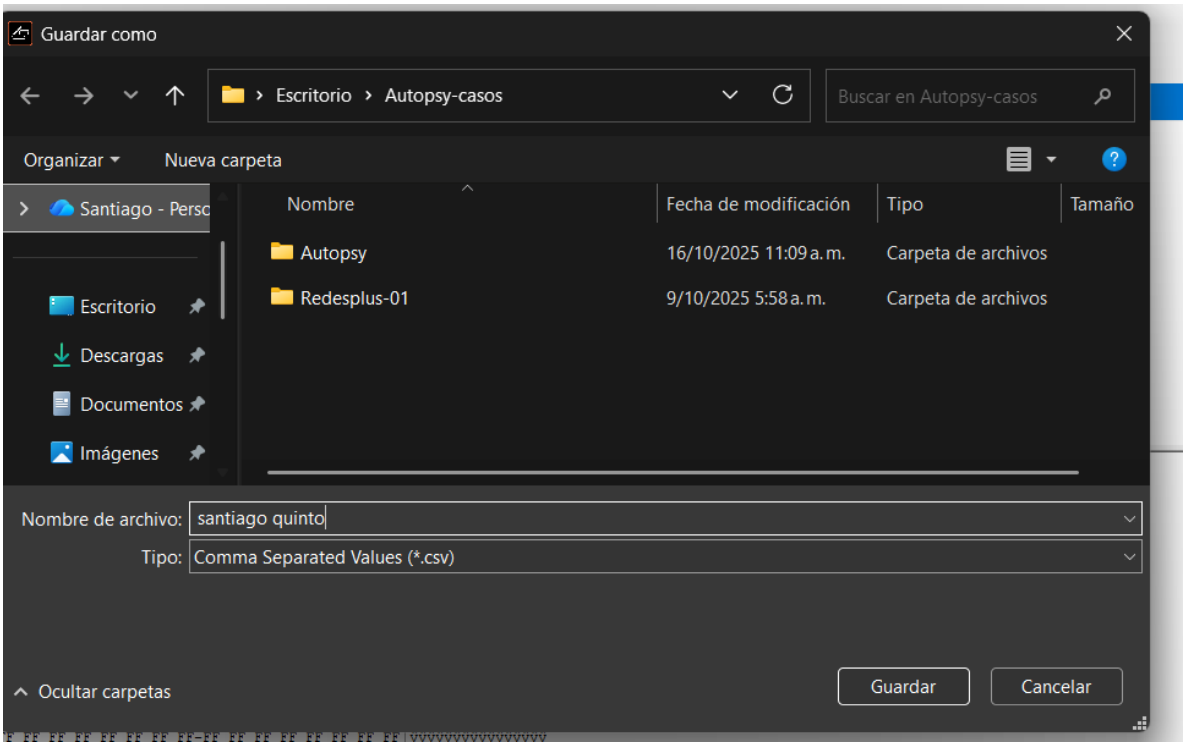


Ilustración 72 Archivos explore en Windows

Esta imagen se muestra una hoja de cálculo de Excel con información forense digital. Contiene hashes MD5 y SHA1, nombres de archivos, rutas de ubicación, sistema de archivos (FAT32) y detalles del volumen analizado. Es útil para verificar integridad de archivos, analizar evidencias y documentar hallazgos en investigaciones informáticas.

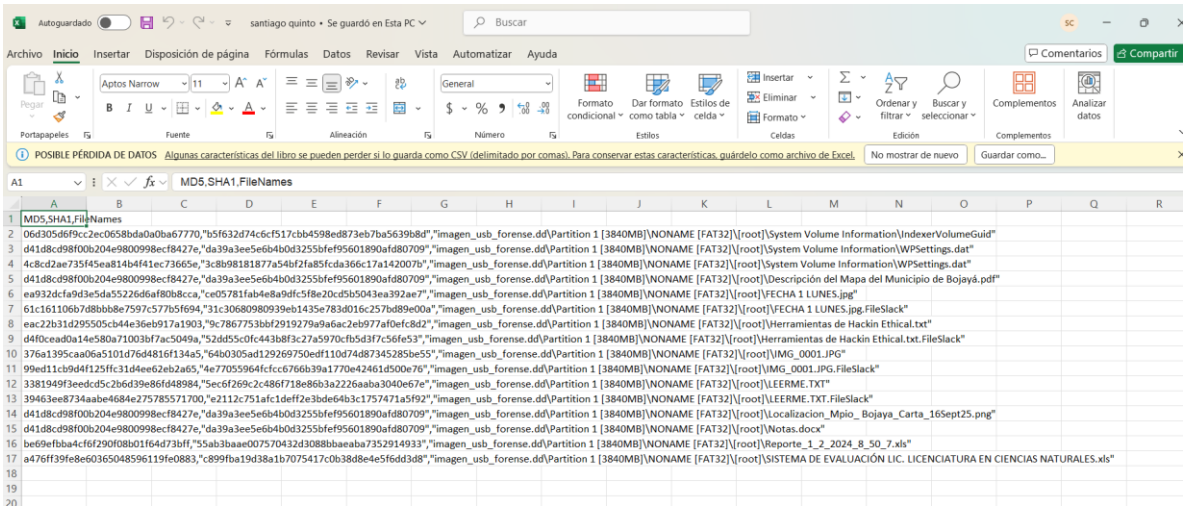


Ilustración 73 almacenamiento seguro del proyecto forense en el Excel.

9 PLANTEAMIENTO DEL PROBLEMA

Durante los procesos de auditoría digital y análisis de incidentes, uno de los principales retos es **preservar la integridad de las evidencias digitales** y realizar un examen técnico sin alterar el contenido original. La manipulación directa de los dispositivos puede generar pérdida de información o comprometer la validez de la prueba.

Por ello, surge la necesidad de emplear herramientas profesionales como **Autopsy** y **FTK Imager**, que permiten crear copias exactas (bit a bit) del medio de almacenamiento, realizar análisis estructurados y verificar la autenticidad mediante valores hash. El problema planteado fue comprobar si las herramientas garantizan la integridad de la evidencia digital y permiten obtener resultados consistentes y verificables.

10 SOLUCIONES

Se utilizó el sistema **Kali Linux** para realizar la identificación y clonación del dispositivo USB mediante comandos forenses (lsblk, fdisk, sha1sum, dd).

Se generó el valor hash **SHA1** para asegurar la integridad antes y después de la copia.

Se empleó **Autopsy** en Windows para realizar el análisis gráfico de la imagen forense, recuperando archivos eliminados, metadatos y registros del sistema.

Se complementó el análisis con **FTK Imager**, verificando la integridad de la imagen, generando nuevos hashes y comparándolos con los originales.

Finalmente, se generaron reportes automáticos de ambas herramientas, consolidando los resultados de la práctica.

11 ERRORES DETECTADOS

- En algunos casos, el sistema **Kali Linux** no reconocía inmediatamente la memoria USB, requiriendo ejecutar nuevamente los comandos de detección (lsusb, fdisk -l).
- Al calcular el hash inicial, se cometieron errores de ruta al intentar guardar el archivo en el escritorio, lo que obligó a ajustar los permisos y directorios.
- En FTK Imager, la primera importación de la imagen falló debido a una extensión incorrecta, que debió ser corregida a .dd.
- Durante el proceso de exportación de reportes, algunas carpetas fueron duplicadas, lo cual se solucionó mediante la organización manual de las evidencias.

12 RECOMENDACION

- Verificar siempre la **ruta de trabajo** antes de ejecutar comandos forenses para evitar pérdida de datos.
- Mantener una copia del **hash original** y compararlo tras cada manipulación de la evidencia.
- Usar **versiones oficiales** de Autopsy y FTK Imager descargadas desde sus sitios originales.
- No trabajar directamente sobre el dispositivo original; siempre hacerlo sobre **copias forenses**.
- Documentar cada paso con capturas de pantalla y registros detallados, cumpliendo los estándares de la cadena de custodia.

13 CONCLUSION

El análisis forense digital realizado con **Autopsy** y **FTK Imager** permitió comprender la importancia de preservar la integridad de las evidencias digitales durante una investigación. A través del proceso, se logró clonar la memoria USB, generar y comparar valores hash, analizar los datos recuperados y validar la coincidencia de resultados entre ambas herramientas.

Las prácticas demostraron que el uso combinado de **entornos Linux y Windows** es eficaz para el tratamiento de evidencias digitales, y que las herramientas aplicadas cumplen los principios fundamentales de la informática forense: **autenticidad, integridad, trazabilidad y documentación**. Con ello, se fortalecieron las competencias técnicas necesarias para desempeñar procesos de auditoría y análisis forense en escenarios académicos o profesionales.

14 BIBLOGRAFIA

RAFAEL SANDOVAL MORALES (2025). Material de apoyo de la asignatura Seguridad y Auditoría de Redes. Universidad Tecnológica del Chocó. (2025).

15 WEBGRAFIA

Autopsy – Descarga oficial:

https://www.autopsy.com/download/

Exterro FTK Imager – Página oficial de descarga:

https://www.exterro.com/ftk-imager

Formulario oficial de registro para FTK Imager 4.7:

https://www.exterro.com/form/ftk-imager-download

Guía externa de instalación – Tecno Sender:

https://tecnosender.com/instalar-ftk-imager-windows/

AccessData/Exterro. (s.f.). FTK Imager. Recuperado de https://www.exterro.com/digital-forensics-software/ftk-imager.

Basis Technology Corp. (s.f.). Documentation - Autopsy User's Guide. Recuperado de https://www.reydes.com/archivos/autopsy_reydes.pdf.